

The impact of the attacks on trust in the use of social media and Service sites in Libya

Radwan M Marwan

Higher Institute of Science and Technology, Tajoura, Libya

it.marwanmr@gmail.com

Abstract

As the use of websites including social media platforms, online financial services, and e-marketplaces continues to grow, so too do the attacks targeting them. Attackers employ a variety of methods, such as phishing, social engineering, spam, Denial-of-Service (DoS) attacks, malware, ransomware, and zero-day exploits. Consequently, there has been a rise in the number of attacks and security breaches affecting users. This research examines these types of attacks and their impact on internet users by gathering data from information technology students at the Higher Institute of Science and Technology in Tajoura and the University of Tripoli. The study aims to determine the frequency and severity of these attacks within our community, measure user confidence when managing accounts amidst such threats, and assess how the impact of an attack varies based on the type of website and platform involved. Furthermore, the study seeks to gauge individuals' awareness and understanding of the risks associated with these attacks, thereby supporting decision-making processes aimed at raising awareness and mitigating the negative consequences of these attacks on society.

Keywords: The Website; Facebook; Attacks on social media; Electronic fraud;

الخلاصة

مع تزايد استخدام المواقع الإلكترونية بما في ذلك منصات التواصل الاجتماعي، والخدمات المالية عبر الإنترنت، والأسواق الإلكترونية تزايدت أيضاً الهجمات التي تستهدفها. ويستخدم المهاجمون أساليب متنوعة، مثل التصيد الاحتيالي، والهندسة الاجتماعية، والرسائل المزعجة (Spam)، وهجمات حجب الخدمة (DoS)، والبرمجيات الخبيثة، وبرمجيات الفدية، واستغلال الثغرات الأمنية غير المكتشفة سابقاً (Zero-day exploits). ونتيجة لذلك، ارتفع عدد الهجمات والانتهاكات الأمنية التي يتعرض لها المستخدمون. يتناول هذا البحث أنواع هذه الهجمات وتأثيرها على مستخدمي الإنترنت، وذلك من خلال جمع بيانات من طلاب تكنولوجيا المعلومات في المعهد العالي للعلوم والتقنية بتاجورة وجامعة طرابلس وبعض المستخدمين من ذوي الخبرة في هذا المجال. وتهدف الدراسة إلى تحديد معدل تكرار هذه الهجمات وشدها داخل مجتمعنا، وقياس ثقة المستخدمين في استخدام حساباتهم عند مواجهة مثل هذه التهديدات، وتقييم كيفية تفاوت تأثير الهجوم على المستخدمين بناءً على نوع الموقع الإلكتروني المعني. علاوة على ذلك، تسعى الدراسة إلى قياس مدى وعي الأفراد وفهمهم للمخاطر المرتبطة بهذه الهجمات، مما يدعم عملية اتخاذ القرار الرامية إلى رفع مستوى الوعي والحد من العواقب السلبية لهذه الهجمات على المجتمع.

Submitted: 03/09/2026

Accepted: 09/10/2026

Introduction

The Internet has become one of the most widely used tools in our daily lives, hosting a vast array of websites that offer diverse services—such as e-commerce, financial transactions, and social media platforms (e.g., Facebook, Instagram, Twitter, WhatsApp, and others). These platforms have gained immense popularity as channels for exchanging information and images, as well as for showcasing and selling products, enabling them to build massive global user bases.

At the same time, users face a variety of cyber threats, including phishing, social engineering, spam, denial-of-service attacks, malware, ransomware, and zero-day exploits. Users can be categorized into two groups: those who benefit from the services these platforms provide, and those who launch attacks and perpetrate fraud against these beneficiaries using various malicious methods. In their engagement with these services—such as e-commerce, money transfers, and social media—users face significant challenges: they seek to utilize these platforms without falling victim to attacks that could compromise their security and undermine their trust in the services. A key challenge lies in establishing trust between users and websites. In Libya, the number of internet users reached approximately 6.13 million in 2024—representing 88.4% of the total population [1]—and is projected to rise to 6.57 million by 2025. A report by Kepios indicated that the total number of social media users reached 500,000, marking a 5.8% increase compared to 2024. Despite the numerous benefits the internet offers, various problems arise due to insufficient awareness and training regarding associated risks and types of attacks; furthermore, the cybersecurity infrastructure remains under development, leaving systems vulnerable to cyberattacks. These security vulnerabilities erode user trust and diminish the sense of safety when using many websites. While some studies have focused on various types of cybersecurity attacks—such as social engineering and phishing—and their impact on the security of online buying and selling, others have concentrated on attacks targeting specific types of platforms or examined security within particular domains, such as financial and social contexts.

Other researchers have focused on the technical aspects of attack impacts—without addressing the human factor or broader institutional repercussions regarding trust—limiting themselves to studying a single type of attack on a specific platform (e.g., social engineering) to measure user trust [9] [12] [18].

Although these studies have covered and clarified certain aspects, there is a need to understand other facets and address these dimensions to comprehend the relationship between platform type and the frequency of breaches. It is also essential to examine the relationship between the level of trust and security perceived by individuals in Libya regarding attacks while using social media platforms, and to measure the correlation between the impact of attacks and the user base of these sites or platforms. Furthermore, this study differs in terms of location and context; Libyan society differs from other societies regarding demographics, education, and culture—aspects not covered in previous papers.

To address these dimensions, this study examines user perceptions regarding social media platforms, e-commerce sites, and buying-and-selling applications in Libya—specifically concerning user numbers in the event of attacks, the impact of attacks on trust and security, and how attacks influence the choice of platform or website.

Based on this premise, the research questions are as follows:

Is there a relationship between exposure to attacks and a loss of the sense of security and trust?

Is there a relationship between the number of platform users and the frequency of attacks?

Is there a relationship indicating the likelihood of a user experiencing a security breach based on the type of platform chosen?

To answer these questions and achieve the research objectives, the following hypotheses were formulated, and the results were analyzed statistically.

Correlation Hypotheses:

Null Hypothesis (H01): There is no statistically significant effect indicating that exposure to attacks impacts the loss of a sense of security and trust.

Alternative Hypothesis (H11): There is a statistically significant effect indicating that exposure to attacks impacts the loss of a sense of security and trust.

Null Hypothesis (H02): There is no statistically significant relationship indicating the likelihood of a user experiencing a security breach based on the chosen platform type.

Alternative Hypothesis (H12): There is a statistically significant relationship indicating the likelihood of a user experiencing a security breach based on the chosen platform type.

Difference Hypotheses:

(H03): There is no statistically significant inverse relationship between the number of platform users and the rate of attack occurrence.

(H13): There is a statistically significant inverse relationship between the number of platform users and the rate of attack occurrence.

Answering this question helps assess user confidence levels when using websites—despite the risk of attacks—identify the specific types of attacks or threats users fear most, and measure the platform's effectiveness regarding the frequency of attacks.

Literature review

There has been a shift characterized by an increasing frequency of attacks launched via social media; attackers have gained a deeper understanding of website vulnerabilities and are increasingly relying on social engineering techniques—alongside other attack methods—to obtain individuals' personal information through third parties. These methods include prompting users to enter specific details—such as a pet's name, residential area, or other data—which allows attackers to reset the victim's password. Given that many people reuse the same password, attackers have recently become more precise and successful in executing their attacks [2]. In a related context, several U.S. organizations—including (Consumer Reports) and the University of Chicago's National Opinion Research Center—conducted surveys among American citizens regarding their experiences with specific types of attacks, such as fraud, the theft of sensitive data, and the spread of viruses via social media platforms. As highlighted in the Microsoft report (Decoding Emergence), the findings revealed that a limited percentage of users had been subjected to attacks involving various forms of phishing messages. [3][4]; this highlights a lack of awareness and understanding among many people in these regions, given the high rate of compromise. Social media platforms served as the primary arena for these attacks, accounting for 74 percent of all cases, while attacks via text messages and email constituted 20 percent, and scams involving mobile applications or phone calls made up 11 percent [5]. This can be attributed to the fact that the majority of users rely on their personal mobile phones to manage their accounts, particularly when conducting financial transactions or using messaging apps. The report also addressed security threats and attacks, revealing that a significant number of users had been subjected to fraud via phone calls and text messages, while others had encountered phishing attempts. Users who frequently conduct financial transactions expressed deep concern regarding these types of threats; we attribute this to a lack of awareness among some users regarding the secure use of their accounts, as many employ weak passwords or reuse the same password across multiple accounts. Furthermore, younger age groups often fail to pay sufficient attention to the risks of attacks or breaches targeting their devices. This reality demonstrates that, despite Facebook's massive active user base, only a small fraction prioritize security policies, leaving a large segment of users vulnerable to compromise. [6] [7] [8]. This global disruption has negative repercussions for user security and trust levels, at both continental and local scales. Recent years have witnessed a surge in the use of communication tools

including social media platforms, money transfer services, and mobile banking applications driving the number of internet users in Africa to over 700 million. Concurrently, however, trust and a sense of security regarding interactions between individuals and institutions particularly concerning financial transactions have declined amidst rising cyberattacks targeting social media platforms and financial services. This trend contributed to a notable 30% increase in trust-related losses due to cyberattacks across Africa in 2025, even though many such crimes go unreported. Consequently, financial losses incurred by African nations due to these attacks which target money transfers and e-commerce totaled US\$3 billion between 2019 and 2025 [2]. Attackers have increasingly exploited security vulnerabilities to perpetrate fraud and phishing attacks especially via social media using social engineering techniques. Phishing attacks are the most prevalent form, enabling attackers to access sensitive information such as passwords and identity details, particularly within the financial sector (banking and e-commerce) and on social media platforms [9] [10] [11] [12]; reports indicate a phishing rate of 34% in Africa. This issue affects numerous companies across the continent, with Egypt and South Africa being the most heavily impacted nations. The report also highlighted the rise of Distributed Denial-of-Service (DDoS) attacks in African countries, with Ghana alone recording 4,735 such incidents. North African nations including Morocco, Tunisia, Egypt, and Algeria experienced a variety of attacks, ranging from mobile application fraud (such as scams on WhatsApp) to social engineering attacks on social media platforms. We attribute this trend to a lack of sufficient user knowledge and awareness regarding these types of attacks a vulnerability that attackers exploit to manipulate victims through various forms of fraud [13]

I have observed that most previous studies focus on the technical aspects of attacks rather than on the psychological impact and financial losses experienced by users and organizations consequences stemming from a lack of awareness regarding the scale and effect of these attacks, as well as the user's ability to select a platform architecture that offers adequate protection. This highlights the importance of understanding how such attacks affect user trust in specific websites within Libya; users there do not exist in isolation from the global, regional, or cross-border cyber threat landscape, particularly given the steady rise in the number of users on social media platforms and in the e-commerce sector.

Impact of Attacks on Users

Social media platforms, including Facebook, are subject to numerous attacks that undermine user trust and account security. Facebook users face risks such as identity theft and unauthorized access to personal information, as attackers extract personal data from their accounts. These attacks are carried out through methods such as stealing passwords via keylogging software, compromising devices to obtain access tokens, or launching phishing campaigns containing deceptive links; clicking these links directs users to pages requesting personal information.[12]

Meanwhile, a study noted that while global rates of security vulnerability exploitation have stabilized, ransomware incidents have risen, with state-sponsored cyberattacks targeting companies for extortion. A significant systemic vulnerability identified in 2024 is "cross-contamination of data," where data stolen from compromised corporate devices included users' personal information and vice versa thereby vastly expanding the scope of social media-related threats affecting user trust and security.[14] Studies indicate that these attacks drive individuals to frequently change their accounts due to fears of data theft and a lack of confidence in platform security; this behavior is further fueled by reports of data breaches and extortion incidents, as well as a lack of full awareness regarding how to activate security tools on these sites. Attackers are increasingly

exploiting security vulnerabilities and employing fraud and phishing tactics particularly via social media platforms by leveraging social engineering techniques [17]. Studies indicate that phishing is the most prevalent type of attack, enabling attackers to access sensitive information such as passwords and identity details, especially within the financial sector (banking and e-commerce) and on social media. These attacks have raised significant concerns regarding the loss of sensitive data and have negatively impacted corporate financial transactions [8][9].

These threats extend to malicious advertising and direct-message scams, utilizing malware capable of altering device behavior to ensure ongoing data exfiltration. By 2025, the financial impact of these threats had reached significant levels for many companies [15][17], often stemming from employees accessing social media via work devices. Beyond financial losses, these attacks cause severe psychological distress and undermine fundamental individual trust.

A study noted that many fraud incidents are linked to mobile applications (such as WhatsApp) and social engineering attacks carried out via social media platforms. These attacks accounted for the largest share of web-based attack incidents in 2024 [13][17]. This has undermined user trust and their sense of security regarding their accounts, leading to a decline in the usage of specific websites. To mitigate these breaches, studies emphasize the necessity of implementing robust protection systems and raising user awareness of security practices an effort platforms themselves can help facilitate. Additionally, providing immediate notifications is crucial to guide users during attacks and minimize their negative impact. Against this backdrop, the study examines user experiences regarding trust following attacks on platforms in Libya.

Trust and Security on Websites

Researchers define trust as the belief that another person can be relied upon, particularly when handling critical situations appropriately [16]. A 2023 literature review on measuring trust in social media content examining relationships between the platform and the user, as well as among users themselves revealed that trust emerges when interactions are grounded in transparency, thereby fostering a sense of security for the other party [17]. Many people currently turn to social media when seeking to purchase goods or acquire products; however, such transactions require meeting several criteria, including persuasiveness, credibility, source transparency, trust, and the availability of a secure payment system [18]. A study addressing concerns regarding security, trust, and privacy in the context of internet and social media usage offered a specific perspective on security concerns: defining them as the extent to which users fear falling victim to fraud, scams, or phishing attacks that could lead to data theft data that may include photos, financial transaction details, card numbers, and other information exploitable by attackers [19]. Meanwhile, privacy concerns have been defined as a user's fear that an attacker might obtain their private data or gain unauthorized access to their personal account [20]. As for trust, we define it as the user's perception of the trustworthiness of the individuals with whom they interact, as well as the reliability of the website or platform itself in ensuring security and preventing unauthorized access to personal data. Finally, we define awareness as the extent of the user's familiarity with the risks and attacks they may encounter while using the Internet and social media; this awareness serves as the cornerstone of user protection.

This study examines attacks targeting various types of websites and analyzes the multiple attack vectors associated with each. It distinguishes itself from previous research through the specific

geographic and cultural context in which it was conducted. Furthermore, the timing of the study is particularly significant given the daily evolution of attack methods. This paper addresses the following questions: Is there a relationship between exposure to attacks and a loss of the sense of security and trust? Is there a relationship between the number of platform users and the frequency of attacks? Is there a relationship indicating the likelihood of a user experiencing a security breach based on the type of platform chosen? Answering these questions helps assess user trust levels—despite the risks of attack—identify the types of attacks or threats users fear most, and understand differences regarding the usability of platforms and websites.

Methodology

This study employed a descriptive research methodology, which is suitable for gathering comprehensive information from participants regarding the types of attacks they encounter while using various websites on computers or mobile devices. These encompassed attacks associated with platforms such as Facebook, YouTube, WhatsApp, and Instagram, as well as threats faced when using online money transfer websites or applications. Information was also collected regarding participants' levels of trust and sense of security while using these sites, alongside data concerning their awareness of different types of attacks and their understanding of the associated risks. The descriptive-analytical approach is particularly useful for measuring and understanding the impact of cyberattacks on the trust and security perceptions of internet users in Libya, as descriptive statistics allow for the assessment of variations in opinions and sentiments across different segments of society. Descriptive statistics allow for the assessment of variations in opinions and sentiments across different segments of society.

Study Population

The study employed a quantitative methodology to ensure statistical accuracy and maintain high research quality. A questionnaire was distributed to students aged 17 to 30 (and older). The participant sample comprised students from the University of Tripoli and the Higher Institute of Science and Technology in Tajoura specifically from Information Technology departments totalling approximately 250 students, alongside 70 experienced web users. Twenty responses 15 from students and 5 from experienced users were excluded due to lack of clarity or internal inconsistency, resulting in a final set of 300 valid responses. These sample sizes are considered sufficient to yield accurate results and statistics. Prior to final distribution, the questionnaire was administered to a pilot group to assess question clarity and gather feedback, thereby ensuring its effectiveness and the reliability of the statistical findings. The sample size was determined based on the minimum requirement of 10 participants per observed variable. Additionally, a random sample of internet users was selected, with a deliberate effort to include IT specialists given their knowledge and usage of these technologies—as well as individuals with relevant professional experience.

Questionnaire Questions:

To address the research question, the study employed criteria designed to ensure statistically significant results; the questionnaire comprised a set of questions aimed at achieving the research objective:

1. Determining the number of users for each website and assessing their level of awareness regarding the types, scope, and severity of cyberattacks;
2. Assessing user levels of trust and security regarding internet software and websites, particularly how this trust diminishes upon exposure to cyberattacks;
3. Measuring the severity of attacks experienced by users on each website; and
4. Measuring the impact of attacks based on the architecture of the platform chosen by the user.

To ensure the questionnaire's validity, various question formats were used, including open-ended questions, rating scales, and multiple-choice questions. The reliability of the research instrument was verified using Cronbach's alpha coefficient to measure internal consistency; the reliability coefficient for the questionnaire items was 0.78. The questionnaire was distributed to students in the Information Technology Department at the Higher Institute of Science and Technology in Tajoura and to students at the University of Tripoli, with a specific focus on the Information Technology Department and the selection of a random sample of individuals on the same day. Following data collection, a Likert scale was applied to the closed-ended questions to determine the general trend of responses, while the standard deviation—calculated at 2.14—was used to measure the variance in responses. Finally, the questionnaire data were digitized and processed using the Python programming language and its available artificial intelligence libraries to analyze the data and derive precise statistics.

The Cronbach's alpha coefficient was used to measure the consistency of the questions.

Number of questions: 12

Number of participants: 300

Sum of question variances: 1.305186

Total variance: 4.5796

$a = (12/11) \times (1 - 1.305186/4.5796)$

$a = 1.090909 \times (1 - 0.285)$

$a = 1.090909 \times 0.715 = 0.78$

Data Analysis

This study evaluates structural differences in user interactions regarding trust, security, and exposure to cyberattack risks as well as the impact of such attacks based on the platform or site type across five major platforms: Facebook, Instagram, WhatsApp, YouTube, and e-commerce websites. A questionnaire was used to assess user perceptions through statistical analysis.

Multi-stage Software Processing:

- Data Definition Phase: Using the (pandas) library, sample distribution is handled by organizing the inputs into a matrix within the analysis framework, based on the questionnaire. size of 300 participants (N = 300).

- Statistical Inference: A Chi-square (χ^2) test is conducted to derive statistical inferences by passing calculated statistics to an evaluation and tabulation module using the (scipy.stats) library.

Statistical Formulas

These processes rely on probability models concerning frequency within a discrete distribution. Questionnaire responses are classified into two categories: a value of "1" indicates the event did not occur, while a value of "2" indicates the event did occur.

Calculating Baseline Rates

Relative frequency equations were used to calculate baseline rates and analyze system usage, website access patterns, and usage reliability, as follows:

Results and Analysis

Figure 1 illustrates the distribution of attacks across websites, the proportion of users for each site, and the distribution of trust in relation to the occurrence of attacks.

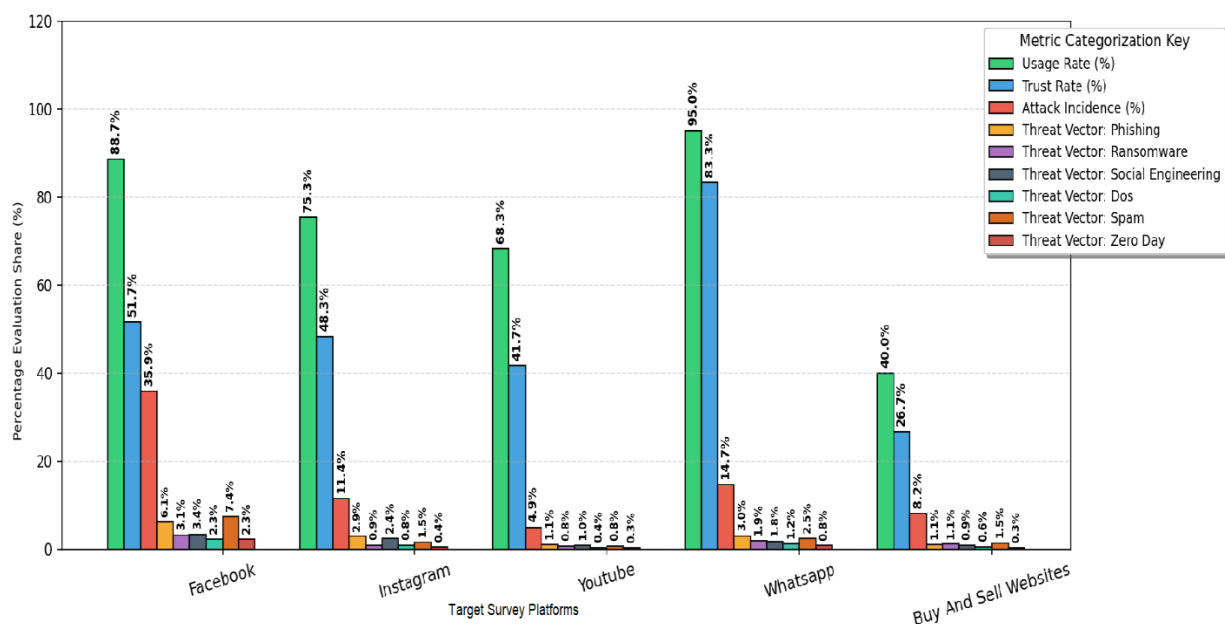


Figure-1: Attacks, Trust, and Usage

Exposure to hacking versus choosing the type of site

Null hypothesis (H_0): There is a statistically significant inverse relationship between the number of platform users and the attack rate.

Alternative hypothesis (H_1): There is no statistically significant inverse relationship between the number of platform users and the attack rate.

The analysis reveals an inverse relationship between platform types and their level of vulnerability to security breaches. Although Facebook and WhatsApp boast high adoption rates amongst users – 88.7 per cent and 95.0 per cent respectively – they differ fundamentally in terms of their susceptibility to compromise; the compromise rate stands at 48.7 per cent for Facebook compared with 14.0 per cent for WhatsApp, highlighting significant differences in their security characteristics.

WhatsApp exhibits the highest level of trust (83.3%) alongside a low-resolution rate (14.7%). In contrast, Facebook faces a rise in the frequency of breaches and an increase in the number of attacks

(35.9%), alongside lower levels of trust and security (51.7%). Consequently, the null hypothesis is confirmed, and the alternative hypothesis is rejected.

We attribute this disparity to the nature of the platforms; open platforms that facilitate widespread interaction – such as Facebook – are more vulnerable to breaches, whilst closed platforms that rely on direct, end-to-end encrypted communication face lower risks.

The reality of attacks targeting the human factor

Empirical data highlights a prevailing trend amongst attackers to use social engineering rather than technical hacking methods. This is evident in the prevalence of social engineering attacks; for example, Facebook scams accounted for 11.3 per cent of incidents, whilst spam messages on the same platform accounted for 8.3 per cent. These figures stand in stark contrast to attacks targeting technical infrastructure such as ransomware and zero-day attacks which each accounted for just 3.3 per cent. An analysis of attack vectors across social media platforms reveals a strong correlation with large-scale, open platforms such as Facebook and Instagram. This confirms that structures designed to maximise user engagement are more vulnerable to social engineering-based breaches, such as manipulation and data theft. The reality of human-centred attacks.

Passive consumption versus transaction-based interaction

YouTube shows a high adoption rate amongst users as high as 68.3 per cent yet records a very low attack rate of 4.9 per cent. This discrepancy is most likely attributable to the platform's one-way content distribution structure, which minimises interactive attacks and direct data exchange between users. In contrast, e-commerce platforms present a completely different scenario; they face a significant challenge relating to trust (26.7 per cent) despite a relatively low volume of attacks (8.2 per cent), which represents the most striking discrepancy in this study. This phenomenon stems from the fact that e-commerce sites which rely on financial transactions – inherently raise concerns and suspicions regarding fraud and phishing, regardless of how low the actual rate of security breaches may be.

Analysis of the chi-square test

This test examines the statistical difference regarding platform breaches based on data representing user responses from a sample of size $N=300$.

Testing the hypothesis regarding the user's choice of platform type:

Null hypothesis (H_0): There is a statistically significant relationship indicating the likelihood of a user being exposed to a security breach based on their choice of platform type.

Alternative hypothesis (H_1): There is no statistically significant relationship indicating the likelihood of a user being exposed to a security breach based on their choice of platform type.

Crosstabulation:

able 1 shows the results of the numbers of attack, where a confirmed breach is coded as 2 and a secure state (no breach) as 1.

Table-1: Recording of Attack Incidents

Empirical Observation Counts	Facebook	Instagram	YouTube	whatsApp	Buy and Sell website	Row Totals
Observed Breached(O_1)	110	30	13	42	23	218
Observed not Breached (O_2)	190	270	287	258	277	1282
Column Sample Totals(N)	300	300	300	300	(300	Ntotal= 1500

Chi-square test analysis

To evaluate the contingency table, we use the chi-square test:

Calculated chi-square value = 159.8670

Degrees of freedom (df): 4 (based on the formula: [number of rows – 1] × [number of columns – 1] = [2–1] × [5–1] = 4)

Approximate significance value (p-value): 1.5611e-33 ($p < 0.001$).

Statistical conclusion

Since the calculated value (1.56×10^{-33}) is less than the standard significance level ($\alpha = 0.05$), we reject the null hypothesis of independence (H_0) and accept the alternative hypothesis (H_1).

There is a statistically significant correlation between the framework, the platform interface and the user profile in terms of vulnerability to attacks. Consequently, the disproportionately high rate of attacks observed on Facebook is a notable characteristic of open social networking sites, rather than merely a random variation in the data.

Comparison of the observed variance with expected values

The deviation of the actual recorded figures from the mathematically expected values reveals statistical significance in the observed data, assuming that all platforms have the same level of security.

Positive deviation for Facebook: whilst Facebook was expected to account for 43.6 per cent of attack cases, 110 cases were actually observed. Assuming complete independence, this indicates a positive deviation, a result of statistical significance. ... This is considered an outlier carrying high risk.

Negative deviation on YouTube: The number of attacks observed on YouTube totalled 13, which is significantly lower than the expected figure of 43.6 per cent. This demonstrates the platform's effectiveness in terms of preventive protection, owing to its architecture based on one-way content delivery.

Logistic Regression Model

Table 2 shows the results of model addresses breach outcomes, assigning a value of 1 to a breach and a value of 0 to a secure state based on a set of predictive variables.

$$\ln(P(Y=1) / (1 - P(Y=1))) = \beta_0 + \beta_1 X_{\text{Instagram}} + \beta_2 X_{\text{YouTube}} + \beta_3 X_{\text{WhatsApp}} + \beta_4 X_{\text{Buy\&Sell}}$$

Table-2: Logistic Regression

Covariate Term(x_j)	Coefficient(β_j)	Standard Error (SE)	Wald x^2	Odds Ratio (e^{β_j})	95% Confidence Interval (CI)
Intercept(β_0) Facebook	-0.5465	0.1198	20.82	1.000	(Reference Group Base)
xInstagram	-1.6508	0.2193	56.67	0.192	(0.125,0.295)
xYouTube	-2.5471	0.3013	71.45	0.078	(0.043,0.141)
xwhatsApp	-1.2690	0.1942	42.71	0.281	(0.192,0.411)
XBuy and Sell website	-1.9427	0.2443	63.23	0.143	(0.089,0.231)

A logistic regression analysis of the dataset (N=300) reveals the following: The reference category 'Facebook' has an odds ratio (OR) of 1.000 and an intercept (β_0) of -0.5465, representing a probability of 36.7 per cent; The odds ratios for the other platforms are compared against this reference level in terms of the risk of exposure to attacks. With regard to the 'isolation effect' within the WhatsApp platform, the odds ratio is 0.281. When comparing WhatsApp to Facebook, we find that WhatsApp's odds ratio is 0.281; which indicates that moving from Facebook's open and interactive platform architecture to WhatsApp's closed architecture results in a 71.9 per cent reduction in the likelihood of exposure to attacks (calculated by subtracting the ratio from 1: $1 - 0.281 = 0.719$), even with an increase in the total number of users. Furthermore, the likelihood of Instagram users being targeted by attacks is 80.8 per cent lower (odds ratio [OR] = 0.192) compared to Facebook users. Although both platforms are owned by the same company, the lower prevalence of hyperlinks in comments on Instagram limits the occurrence of attacks such as spam and phishing. The analysis shows that YouTube (YouTube) is the least vulnerable platform, with a 92.2 per cent lower likelihood of exposure to attacks (odds ratio [OR] = 0.078) compared to 'Facebook'; this demonstrates that one-way platforms – characterised by lower levels of user interaction – are less susceptible to attacks.

Testing the Hypothesis on User Trust Pearson's correlation coefficient (r) was used to assess the relationship between user trust and the frequency of attacks on the platforms they use. The hypotheses were formulated as follows:

Null hypothesis (H_0): There is no statistically significant effect of exposure to attacks on the loss of a sense of security and trust.

Alternative hypothesis (H_1): Exposure to attacks has a statistically significant effect on the loss of a sense of security and trust.

The results indicate a weak positive correlation that is not statistically significant, with $r(3) = 0.16$ and $p = 0.80$. As this p-value is well above the significance threshold of $\alpha = 0.05$, the null hypothesis (H_0) was not rejected; instead, the alternative hypothesis (H_1) was rejected, as no statistical evidence was found to suggest that attacks affect users' trust in using accounts on platforms and the internet. Table 3 shows the relationship between user trust and the frequency of attacks.

Table-3: the relationship between trust and attacks.

Platforms/website	Usage Rate (%)	Trust Rate (%)	Attack Rate (%)
whatsApp	95.0%	83.3%	14.7%
Facebook	88.7%	51.7%	35.9%
Instagram	75.3%	48.3%	11.4%
YouTube	68.3%	41.7%	4.9%
Buy and Sell website	40.0%	26.7%	8.2%

Discussion

Statistical analysis revealed no correlation between cyber-attacks and the level of trust in the use of online platforms and websites. This shows that trust remains intact despite the limited number of attacks, a trend observed in general user behaviour. This is clearly evident in the case of Facebook, where we observe a high attack rate of 35.9 per cent; however, this is accompanied by a usage rate of around 88.7 per cent and a strong level of trust at 51.7 per cent, which indicates an inverse relationship between the number of platform users and the attack rate. These figures suggest that the benefits reaped by individuals and organisations such as communication, the exchange of information and financial gains far outweigh the threats posed by these attacks. In contrast, the WhatsApp app which operates in a more closed environment shows a different pattern; it records a confidence level of 83.3 per cent, a usage rate of 95.0 per cent and an attack rate of 11.4 per cent. YouTube, meanwhile, has the lowest breach rate at 4.9 per cent, with a trust level of 41.7 per cent. These figures demonstrate that measuring trust and security is not merely a matter of conjecture, but is based on statistics that reflect the perceptions of individuals and organisations; as a result, users place greater trust in WhatsApp which utilises end-to-end encryption compared to Facebook. This suggests a correlation indicating the likelihood of a user being exposed to a security breach based on their choice of platform. As for 'YouTube', despite the low rate of breaches on the platform, users remain sceptical about certain external content, even though the platform is safer than others. Finally, e-commerce platforms and online marketplaces show mixed figures: a usage rate of 40.0 per cent (which is considered low), a trust level of 26.7 per cent, and an attack rate of 8.2 per cent. This pattern is attributed to feelings of fear and caution associated with financial transactions, which may require users to share sensitive data, such as payment card details and other personal information.

Conclusion

This study focused on identifying the user base of specific websites, the types of attacks targeting them, and the impact of these attacks on user trust. The results revealed a lack of user knowledge and awareness regarding attack types, leaving accounts vulnerable and raising concerns; in some instances, this even led to diminished trust in using certain sites. WhatsApp and Facebook topped the list of most-used platforms with comparable usage rates (95.0% and 88.7%, respectively); however, Facebook was more susceptible to attacks (35.9%) and commanded lower user trust (51.7%), as many users fell victim to social engineering and phishing tactics. Nevertheless, user trust remained resilient; the study indicates that security breaches and attacks did not fundamentally undermine the confidence of those affected—a trend particularly evident with Facebook. In

contrast, WhatsApp was less vulnerable to attacks (14.7%) and enjoyed higher levels of trust (95.0%). For other sites like YouTube, usage and trust rates were comparable, suggesting that open social platforms (such as Facebook) are more exposed to risks than those with more restricted communication structures (such as WhatsApp and YouTube), despite some occasional variations. Regarding e-commerce sites and financial applications, although they faced lower attack rates, usage and trust levels were also low. This reflects users' apprehension about sharing personal and financial data online particularly with unknown parties—which in turn increases their vulnerability to various types of attacks. However, the benefits offered by many websites such as information exchange and access to diverse content ultimately prompt users to look past the risks of cyberattacks and focus on the significant advantages available, thereby maintaining user confidence despite the persistent threat of attacks.

Recommendations

This section focuses on informing users of the steps they should take to ensure the security of their online accounts.

- The role of the responsible authorities and specialists must be more effective in raising public awareness of the risks of cyberattacks and explaining the different types of attacks. This should be achieved through training courses, workshops and seminars, as well as public announcements.
- Users must not provide their personal details to unknown parties or to certain websites that send forms and request them to be filled in.
- Among the essential items that must be installed on their devices are antivirus software and security programmes, such as those that lock certain ports on the device.
- Users should exercise caution when dealing with online marketplaces and should not transfer funds until they have verified the site's credibility, as there are many fraudulent sites.
- Websites should enhance their security levels whilst providing user-friendly tools for securing their sites. This is due to the varying levels of user proficiency in using these tools, particularly among those with little knowledge of cybersecurity.
- There are numerous security features on websites, and with security tools available, users must be aware of them and activate them when using their accounts.
- Users should not log in with people they do not know and should not click on any image, link, programme or email sent to them by someone they do not know, as these may be malicious programmes designed to take control of your device.
- Users should not use weak passwords; passwords must consist of symbols, numbers and letters. Furthermore, the same password should not be used for more than one account.
- Users should choose trusted browsers and be aware of and apply the security policies they offer, which prevent malicious software from accessing your device and block certain dangerous vulnerabilities.

References

- [1] A. S. I. Mohmed, “Analyzing Barriers to the Adoption of Websites and Mobile Applications in Libya : A Mixed-Methods Study on E-Services , Trust , and Digital Transformation,” vol. 2, no. 2, pp. 74–83, 2025.
- [2] INTERPOL, “Interpol Africa Cyberthreat Assessment Report 2025,” no. May, pp. 30–33, 2025, [Online]. Available: <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa>
- [3] Consumer Reports, Aspen Digital, and Global Cyber Alliance, 2026 Consumer Cyber Readiness Report. Oct. 1, 2026. [Online]. Available: <https://www.aspendigital.org/report/2026-consumer-cyber-readiness-report/>
- [4] Microsoft Threat Intelligence, “Decoding Emergence,” in Microsoft Digital Defense Report 2026. Microsoft, Oct. 1, 2026. [Online]. Available: <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/2026-digital-defense-report>
- [5] 2021“BITDEFENDER GLOBAL REPORT: CYBERSECURITY AND ONLINE BEHAVIORS,” 2021.
- [6] A. Naz, M. Sarwar, M. Kaleem, M. A. Mushtaq, and S. Rashid, “A comprehensive survey on social engineering-based attacks on social networks,” *Int. J. Adv. Appl. Sci.*, vol. 11, no. 4, pp. 139–154, 2024, doi: 10.21833/ijaas.2024.04.016.
- [7] Vedashree Takalkar and Parikshit Mahalle, “Handling Data Confidentiality Attack due to Data Sharing using Trust-based Approach in Online Social Networks,” *Int. J. Eng. Res.*, vol. V4, no. 05, pp. 122–125, 2015, doi: 10.17577/ijertv4is050151.
- [8] S. Kulkarni, “Cyber Security: Types of Attacks,” *Int. J. Eng. Res. Comput. Sci. Eng.*, vol. 11, no. 6, pp. 2394–2320, 2024.
- [9] A. Jafar, A. Yeboah-Ofori, T. Abisogun, I. Hilton, O. Oguntolayinbo, and O. Oyetunji, “The Impact of Social Engineering Attacks on the Metaverse Platform,” *Proc. - 2024 11th Int. Conf. Futur. Internet Things Cloud, FiCloud 2024*, pp. 201–208, 2024, doi: 10.1109/FiCloud62933.2024.00038.
- [10] G. Bergmanis-Korāts, T. Haiduchyk, and B. Smolts, *Social Media Manipulation for Sale: 2025 Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement*. Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2026. [Online]. Available: <https://stratcomcoe.org/publications/social-media-manipulation-for-sale-2025-experiment-on-platform-capabilities-to-detect-and-counter-inauthentic-social-media-engagement/338>
- [11] P. Ankush Bhoite and S. Ravindra Desai, “Cyber Security Risks in Social Media,” *Int. J. Creat. Res. Thoughts*, vol. 14, no. 5, pp. 554–560, 2026, doi: 10.56975/ijert.v14i5.308388.

- [12] S. A. Talib, "Cybersecurity in Social Media," *Al-Rafidain Journal of Engineering Sciences*, vol. 3, no. 2, pp. 132–140, 2025, doi: 10.61268/zwxnbnm29.
- [13] C. S. Parr, "Does social media undermine trust? Institutional trust in civil society and governance institutions," *J. Public Policy*, pp. 737–760, 2025, doi: 10.1017/S0143814X25100834.
- [14] The Verizon DBIR Team, "2025 Data Data Breach Breach Investigations Report Report," p. 115, 2025, [Online]. Available: <https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf>
- [15] M. I. Hossain, "Exploring the Impact of Social Media on Cybersecurity Threats and Mitigation Strategies," *ResearchGate*, Sep. 2025. [Online]. Available: https://www.researchgate.net/publication/395339633_Exploring_the_Impact_of_Social_Media_on_Cyber_security_Threats_and_Mitigation_Strategies
- [16] A. Thamanna and R. Subramani, "Impact of Social Media Usage on Relationship Development among female college students: The Mediating role of trust," *Observatorio*, vol. 19, no. 2, pp. 91–110, 2025, doi: 10.15847/obsOBS19220252537.
- [17] D. Srivastava, B. Rathore, R. Kumari, S. Das, and V. Goel, "The Role of Social Media Dependence and Social Influence in Shaping Consumer Trust and Purchase Intention," *J. Mark. Soc. Res.*, vol. 2, no. 3, pp. 108–116, 2025.
- [18] A. Koohang, K. Floyd, J. Yerby, and J. Paliszkievicz, "Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument," *Issues Inf. Syst.*, vol. 22, no. 2, pp. 133–145, 2021, doi: 10.48009/2_iis_2021_136-149.
- [19] J. Jamin, N. A. Md Arifin, S. A. Mokhtar, N. N. I. Nik Rosli, and A. I. Mohd Shukry, "Privacy Concern of Personal Information in the Ict Usage, Internet and Social Media Perspective," *Malaysian E Commer. J.*, vol. 3, no. 2, pp. 15–17, 2019, doi: 10.26480/mecj.02.2019.15.17.
- [20] A. Farooq, J. Salminen, J. D. Martin, K. Aldous, S. G. Jung, and B. J. Jansen, "Exploring Social Media Privacy Concerns: A Comprehensive Survey Study Across 16 Middle Eastern and North African Countries," *IEEE Access*, vol. 12, no. July 2024, pp. 147087–147105, 2024, doi: 10.1109/ACCESS.2024.3463869.