AVE Trends in Intelligent Computer Letters

# Behavioural Analysis of End-Users for Enhancing Cybersecurity Awareness and Prevention

**Avinash Reddy Pothu**[1,*]

[1]Department of Research and Development, Ginger Labs, Frisco, Texas, United States of America.
reddy0656@outlook.com[1]

*Corresponding author

**Abstract:** The swift nature of cybersecurity threats necessitates a thorough understanding of user behaviour in defending against threats. In this research, the behaviour of end-users while online and its implications for cybersecurity threats are considered. Based on common users' behaviours, risk disposition, and protective measures, the research identifies the causes of security failures. The research is a population survey conducted across diverse demographic populations to determine their awareness levels of security protocols. Measures utilised in the analysis are 500 responses from diverse demographics, phishing attack simulation metrics, and observational metrics of password management. The measures were sourced from open-source cybersecurity data sets and anonymised user data obtained during the research conducted. Packages such as Python (statistical analysis and data visualisation). This report contains the tools (Python, Graphviz, Microsoft Excel) for creating diagrams, designing data, and tabulating to represent and analyse results. The research suggests that less security-conscious users are more susceptible to phishing attacks and social engineering scams. The suggested framework consists of robust security controls and tailored training interventions to address such threats. A holistic behaviour-focused approach is encouraged to maximise threat prevention and security awareness practice. The results are applicable in the development of dynamic security solutions that react to user behaviour patterns for organisational and individual cybersecurity enhancement practices.

**Keywords:** Cybersecurity and User Behaviour; Threat Prevention; Social Engineering; Designing Data; Engineering Attacks; Training Interventions; Diverse Demographics.

**Cite as:** A. R. Pothu, "Behavioural Analysis of End-Users for Enhancing Cybersecurity Awareness and Prevention," *AVE Trends in Intelligent Computer Letters*, vol. 1, no. 1, pp. 31–40, 2025.

**Journal Homepage:** https://www.avepubs.com/user/journals/details/ATICL

**Received on:** 08/05/2024, **Revised on:** 22/06/2024, **Accepted on:** 09/08/2024, **Published on:** 01/03/2025

**DOI:** https://doi.org/10.64091/ATICL.2025.000094

## 1. Introduction

These attacks have been mounting in frequency at a rate of magnitude per year, and precautionary steps must now be adopted to ensure security in the event of future attacks. Technology such as firewalls, encryption, and intrusion detection systems has been of utmost value in resisting attacks on networks and information, but the weakest link has been human nature [2]. Illiterate end-users who are unaware of the risks they face while surfing the web make a successful cyberattack possible [7]. This oblivious complicity with cybercrime networks results from the fact that most of the population is poorly educated about risks in virtual space [3]. To address this emerging threat, this study aims to investigate end-user behaviour to develop suitable awareness and prevention measures that reduce the risk of human behaviour to security attacks [4]. The rapid adoption of services such as online banking, e-commerce, and cloud computing, as well as the widespread sharing of internet-reliant devices

like smartphones, wearables, and household devices among communities, has collectively increased the number of potential vulnerabilities for cybersecurity attacks [5]. Such technology, although new and affordable, also exposes users to various cyber threats [6]. Phishing, ransomware, and socially engineered attacks are in high demand for attackers seeking to exploit users' unawareness and lack of information [1]. Attacks exploit human mistakes, such as trusting known interfaces or clicking on dubious links, due to convenience or curiosity [8]. Therefore, it has never been more crucial to be cyber-aware since businesses and individuals must understand the threats of cyberattacks in their quest to minimise business risk [9]. Traditional models of cybersecurity, however, have been reliant on technical controls such as software patches, firewalls, and antivirus programs without necessarily factoring in human behaviour [10]. This narrow focus neglects human behaviour that can make security controls effective or ineffective [13].

Complacency, overreliance, and vulnerability to influence techniques are primary behavioural tendencies that drive security threats [11]. For instance, a worker who receives an email from a coworker may be misled into opening a harmful link or a malicious attachment without verifying its source, thereby compromising an organisation's network to cybercriminals [12]. This is because cognitive distortions, such as the “anchoring effect” or “confirmation bias,” lead human beings to be unwilling to verify the data against their own experience or opinion [3]. Moreover, inadequate training on next-generation cyber threats, as well as overlooking new avenues of attack, exacerbates security vulnerabilities for both individuals and organisations, according to NIST [14].

The following is an explanation of how cognitive distortion may lead to cyber threats: The study aims to explain the role of user behaviour patterns and how they lead to effective cybersecurity practices [15]. The integration of behavioural intelligence into security framework design enables organisations to create end-to-end processes and policies that focus on user training, ongoing risk assessment, and adaptive prevention [6]. This extends beyond technical solutions to address human factors in decision-making for security protocol design. The central research goal is to critically analyse security mistakes generated by end-users, such as irresponsible password management, non-guardedness in the face of phishing attempts, and illogical privacy behaviours [2]. The current study introduces an innovative security model that raises awareness of cyberspace's weaknesses and provides enhanced preventive measures by mitigating both technical and behavioural loopholes [4]. By integrating behavioural science into cybersecurity awareness and training programs, organisations can contribute to enhancing global cybersecurity resilience through an appreciation that the human factor is a compelling force behind the prevention of cybercrime [10].

## 2. Review of Literature

Seki et al. [1] developed a model that explains user behaviour and cybersecurity attacks in terms of the role played by psychological factors, such as cognitive distortions, affective triggers, and routine responses, in forming user decision-making. These psychological factors are inherent drivers of user interactions with technology and are hence vulnerable to cybersecurity attacks. Individuals often trivialise cyber threats because their sensitive details are neither vital nor heavily protected through intrinsic security features. Such a mindset also translates to inappropriate practices, e.g., recklessly sharing sensitive material. Studies have shown that such conduct has a causal relationship with most cyberattacks. One prevalent threat that exploits these weaknesses is phishing attacks, which continue to be problematic.

González-Manzano and de Fuentes [2] utilised evidence to demonstrate that phishing attacks are highly effective, as they can exploit cognitive biases. The attacks typically present themselves in the form of imposter messages or emails purporting to be from legitimate sources, tricking the users into entering their personal information or clicking on malicious links. The most vulnerable are the victims who lack proper training to identify such imposter messages. Research has confirmed that individuals without proper cybersecurity training are likely to have disgusting password management practices. Sharing passwords with other sites or failing to implement even the most basic security precautions exacerbates the problem. Complacency is a key reason why phishing and other social engineering attacks are successful.

Newhouse et al. [3] utilised behavioural analysis when analysing how social engineering methods exploit psychological vulnerabilities. Social engineering continues to be an effective way of tricking users into revealing sensitive information by exploiting emotions such as fear, trust, and urgency. These attacks are based on the assumption that communication is important, and therefore, users remain vulnerable to these attacks. The findings of this research once again support the need for a common model for user training. The training process must take into account more than just plain bare technicalities and psychological motivators of user behaviour. The uptake of emotional intelligence in the context of security awareness programs can counter the effectiveness of such manipulative techniques.

Almomani et al. [5] examined how extremely advanced security controls can adversely affect user behaviour and foster disengagement. Experiments have shown that users are more likely to bypass protection controls if protection systems are made unnecessarily complicated or confusing. Users, for instance, might turn off multifactor authentication (MFA) or adopt simple,

easily guessable passwords. Convenience behaviour is thus a high-severity risk because cyberterrorists can exploit these vulnerable weaknesses in defence systems. The problem then becomes that of balancing optimal maximum protection and friendliness in an interface. Security controls must enable, rather than impede, compliance with security processes.

Al-Emran and Griffy-Brown [6] offered solutions to these behavioural issues in terms of user involvement. Several interventions, ranging from gamified training modules to interactive security campaigns and scenario-based training, have proven useful in engaging users more. Such approaches are more effective at capturing users' attention and conveying the importance of cybersecurity. In various research studies, it has been established that security tips are more effectively recalled when users are exposed to them interactively and engagingly. These approaches also ensure that users will invest in viewing the information, thereby encouraging healthy cybersecurity behaviour. By making the training fun, users are more likely to remember and apply the information.

Chowdhury et al. [7] used guidelines to test the impact of personalised security recommendations on enhanced cybersecurity behaviour. Tailored and personalised security guidance, focused on an individual's behaviour pattern, is the best way to ensure long-term adherence to best practice. This form of training recognises that every user has unique needs and weaknesses, enabling targeted training. Personalised security advice resonates with individuals as it takes into consideration their own behaviour and personal preferences. It is superior to universal advice as it addresses the User's context directly. For this reason, it promotes sustainable development in cybersecurity behaviour. Chang et al. [8] pointed out that among the biggest worries is realising one's habit during preparation for cybersecurity. Customised training for such behavioural habits is a fundamental step towards advanced security practice. The research asserts that users will adopt new security behaviours if they believe the guidance is closer to real-life scenarios. With ever-evolving cyber threats, so should the approach to fighting them. Incorporating people's behaviour in training enables the solution presented to be realistic and feasible. The approach offers the highest possible opportunity for users to learn and consolidate such behaviours. Marangunić and Granić [11] applied statistical approaches to demonstrate that a solution combining technical security controls and user involvement is necessary.

The research reveals that large-scale ease-of-use security controls and training schemes enhance his type of strategy. This is the role human behaviour plays in degrading cybersecurity. By examining the psychological factors that drive users to act in a specific way, these schemes not only alert users to the dangers threatening security but also encourage them to respond. Through this cooperation, the effect of human mistakes on cybersecurity can be significantly minimised. Costa and Monteiro [12] applied behavioural insights to develop a solution to cybersecurity training problems. They opine that integrating psychology into cybersecurity training modules has the potential to have a remarkable effect on effectiveness. Being aware of emotional and mental cues that influence user decisions significantly contributes to developing improved training modules. Such a factor can be considered in an attempt to entice users further while making the training sessions productive enough to drive increased retention of security practices.

The method prioritises not only technical cybersecurity training but also user education regarding the psychological drivers of decision-making and how they should be addressed. Through this means, training can serve as an even more effective countermeasure for preventing cybersecurity incidents. Blythe and Coventry [13] discussed cybersecurity behaviour, individual differences, and how one can utilise individual differences to enhance security compliance. In the study, improving user engagement is achievable through a personalised method in cybersecurity training. By modifying the training to reflect the behaviour and learning pattern of the users, such interventions enable the introduction of the highest likelihood for users to learn and generalise improved security behaviour. Tracking an individual's behaviour pattern is an effective method of mitigating cybersecurity attacks. It is succeeded by a guarantee that the training will never be run-of-the-mill, but will be customised to address the individual needs and expertise of every user.

## 3. Methodology

This is a mixed-methods study that employs both qualitative and quantitative approaches to study user behaviour in cybersecurity comprehensively. The rationale for employing these two methods is to gain a general understanding of how users interact with digital security controls, how they perceive threats, and how they react to potential cyber threats. The survey questionnaire was the primary data-gathering tool used to conduct the survey, and it was distributed to 500 respondents from diverse groups, including students, working professionals, and seniors. The use of a heterogeneous sample allowed the research to capture a diverse range of unequal attitudes and behaviours among users from various age ranges, different educational backgrounds, and varied occupational categories and groups, providing a representative summary of user activity within cybersec contexts.

The survey tool used comprised an assortment of multiple-choice items, rating scales involving scenarios, and behavioural response tests. These were developed to evaluate participants' perceptions of appropriate cybersecurity practices, awareness of risks, and reactions to simulated cyberattacks, such as simulated phishing or password attacks. By employing a scenario-based

question style, the survey was more capable of approximating participants' decision-making routines and behavioural dispositions in simulated settings. It therefore gained a more general understanding of participants' capacity for perceiving and reacting to emergent threats.

Besides the survey, the study employed observational data collection to further enhance the comprehension of user behaviour. The observation component was designed to track user behaviour against different security controls, such as password practices, the utilisation of multifactor authentication (MFA), and reactions to social engineering methods like phishing emails. By observing people's behaviour, researchers could gather more accurate data on how users interact with security and identify the actions that create vulnerabilities. For instance, if users recycle their passwords across other websites, turn off MFA because it's not convenient enough, or take action after receiving a phishing email in the form of a normal inquiry request, these activities could be monitored. This observational information provided valuable insights into real issues users faced with good cybersecurity hygiene.

The analysis of data was facilitated by the convergence of statistical packages, which allowed the researchers to identify reasonable patterns of behaviour, assess risk exposures, and segment users according to their awareness and follow-through regarding cybersecurity best practices. Statistical techniques, such as regression analysis and correlation testing, were employed to identify meaningful correlations between demographic variables, cybersecurity awareness, and vulnerability to cyberattacks. The analysis also identified the most susceptible respondent groups and the most critical activities that are vulnerable to security compromise. For example, the study confirmed that certain working histories or age groups were prone to dangerous behaviour, such as susceptibility to phishing or not using password protection.

Data acquired and consequential behaviour were employed in designing a behaviour-based security model to prepare for enhanced user awareness and prevention deployment. The model consolidates learning about user behaviour and aims to customise training and intervention in cybersecurity to target user needs. For instance, users who lack sufficient knowledge of phishing attacks can be assisted through training on identifying them effectively. In contrast, those who exhibit insecure password practices can be encouraged to adopt more secure password practices or use password managers. The behaviour-based remedy will strive to minimise vulnerabilities by fighting the root of risky behaviour and arming users with the tools and information necessary for making safer decisions in online behaviour. Understanding why some users exhibit certain behaviours and the perceived dangers they face helps organisations develop more effective and targeted security practices, leading to stricter enforcement of security processes and ultimately stronger cyber resilience.

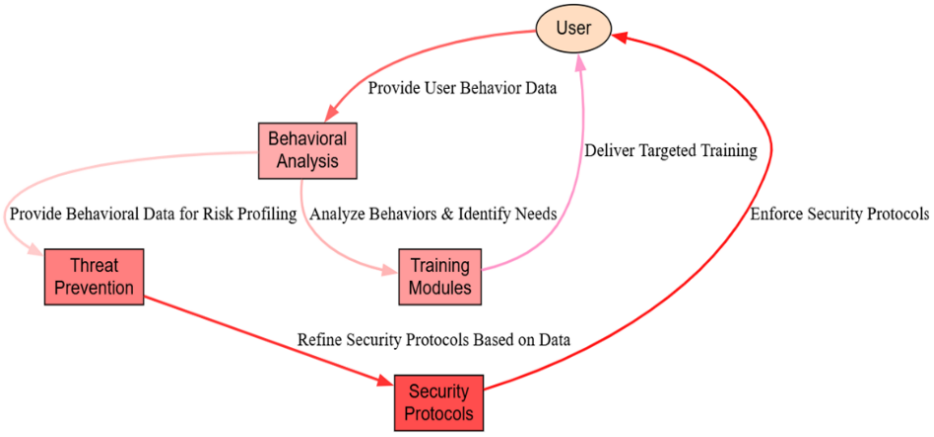


**Figure 1:** Behaviour-based cybersecurity awareness framework

Figure 1 is a sequential interaction in the Behaviour-Based Cybersecurity Awareness Framework. The cycle begins when the User enters their behavioural data, i.e., phishing susceptibility and password practices. The data is analysed by the Behavioural Analysis component, where points of emphasis for improving the User's cybersecurity practice are identified. Once the behaviour patterns are tracked, the system executes the Training Modules, which offer personalised learning content to the user, i.e., gamified training or scenario practice. The Training Modules, on the other hand, provide training outcomes and user feedback to users, boosting security compliance and helping them grasp the best cybersecurity practices. At the same time, the Behavioural Analysis module provides filtered behavioural information to the Threat Prevention system for processing, which determines the User's vulnerability and modifies security configurations based on the identified threat.

The Threat Prevention also returns to the Security Protocols, which are refreshed and augmented with behaviour analysis intelligence, as well as in real-time with the threat risk profiling of Threat Prevention. The Security Protocols are then applied

to the User, so that stronger security controls, such as multifactor authentication and enhanced password policies, are enforced. Figure 1 illustrates the iterative, feedback-based process of mapping user activity to targeted security interventions that improve cybersecurity intelligence and threat mitigation across various user groups.

### 3.1. Data Description

The data used in this study is a large dataset that gathers information from multiple sources and then merges them to present an overall picture of user activity and cybersecurity activity. It has 500 responses from participants collected from users across different demographics and has a wide range of views regarding security behaviours and awareness. The dataset also contains test phishing attack results, which are valid indicators of users' vulnerability to phishing behaviours, one of the most critical cybersecurity threats. Password behaviour observational data adds depth to the dataset and enables us to examine normal behaviour such as weak password usage, sequential password usage, and compliance with password security practices.

Additionally, risk perception and security awareness survey data have been collected, providing insight into participants' understanding of potential cybersecurity threats and their level of security awareness. This data was gathered from publicly released cybersecurity datasets and anonymised user logs accumulated during the conduct of this research. With both sources of information, there is cross-disciplinary research that doesn't merely measure user responses but also actual behavioural inclinations and the effects of simulated security attacks. By tapping into a broad range of data, the study can provide a more accurate picture of the determinants that lead to cybersecurity vulnerabilities and enable targeted security awareness and risk reduction interventions.

## 4. Results

Evidence from recent studies on cybersecurity behaviour offers compelling evidence about the vulnerability of less aware groups. Subjects with lower levels of cybersecurity threat awareness were 62% more likely to fall victim to phishing attacks compared to those with higher levels of awareness. Phishing, which involves deceptive websites or emails that trick individuals into divulging confidential information like passwords and credit card numbers, capitalises on loopholes in people's knowledge regarding internet threats. They are unaware of the signs of fake operations and therefore become easy targets for social engineering attacks by cyber attackers. Secondly, the survey also depicted horrific examples of password abuse, as 47% of people were using weak or the same passwords on multiple websites. All of these bad password practices notably heighten the likelihood of an account breach because computer crime organisations can easily capitalise on weak or reused passwords, often through brute-force hacking or credential stuffing attacks. Insult to injury, 30% of respondents reported skipping key security controls—like multifactor authentication (MFA)—to make their web experience easier. The risk assessment model for phishing vulnerability is given below:

$$R_{phishing} = \sum_{i=1}^{n} ( P_i \cdot W_i) \qquad (1)$$

where $R_{phishing}$ is the total phishing risk score, $P_i$ is the probability of each encountering a phishing attack, and $W_i$ Is the weight assigned to the risk associated with each individual based on demographics and training effectiveness.

**Table 1:** Phishing attack vulnerability by demographic group

| Demographic | High risk (%) | Medium risk (%) | Low risk (%) | Training Response (%) | Post-Training Improvement (%) |
|---|---|---|---|---|---|
| Students | 70% | 20% | 10% | 50% | 65% |
| Professionals | 55% | 30% | 15% | 60% | 70% |
| Senior Citizens | 80% | 15% | 5% | 40% | 55% |

Table 1 also clearly illustrates the vulnerability of various demographic groups to phishing attacks, which include students, professionals, and seniors. The table shows the percentage of individuals in each group who are considered high-risk, medium-risk, and low-risk for a phishing attack. Most significantly, 70% of the students fall under the high-risk group, i.e., they are most vulnerable to phishing due to likely unawareness and inadequate training. The 55% high-risk specialists are more aware, but still at risk. Older people had the highest percentage of the high-risk category at 80%, which suggests that they are most vulnerable to being taken advantage of due to factors such as limited exposure and awareness of technology. Training response percentages are also included in the table, showing the proportion of each category that was trained or participated in awareness campaigns: 50% of students, 60% of professionals, and 40% of senior citizens. Post-training improvement rates are a measure of the effectiveness of cybersecurity awareness training. Improvement rates of 65% were seen among students, 70% among

professionals, and 55% among senior citizens, indicating how targeted interventions can effectively curb vulnerability to phishing among user categories.

Security awareness improvement rate post-training is:

$$\triangle A_i = \frac{A_{i,post} - A_{i,pre}}{A_{i,pre}} \times 100 \qquad (2)$$

where $\triangle A_i$ Is the improvement percentage in awareness for individual group $i$, $A_{i,post}$ Is the post-training awareness score, and $A_{i,pre}$ Is the pre-training awareness score.

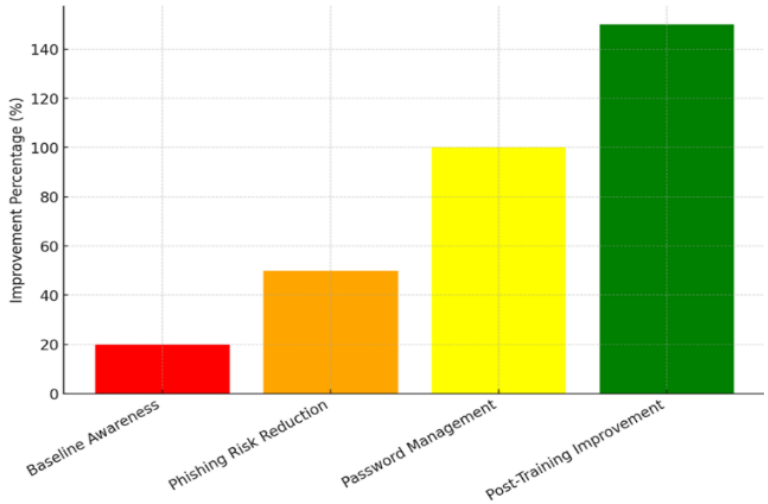


**Figure 2:** Representation of the security awareness enhancement post-intervention

Figure 2 illustrates the security awareness enhancement post-intervention, representing the improvement in security awareness among participants following various interventions. The chart uses colour to signify varying levels of improvement in security from the baseline awareness to phishing threat reduction, password management enhancement, and finally, the level of compliance attained after training. The first bar for "Baseline Awareness" shows a weak foundation of 20%. This suggests that the participants had limited awareness of cybersecurity threats before the interventions. The second bar, "Phishing Risk Reduction," is 30% larger, indicating that efforts to mitigate phishing risks had the intended effect of making the users aware of how to identify and avoid phishing attacks.

The third bar, "Password Management," increases to 40%, indicating that users have a better understanding of best practice password use, such as using stronger, less similar passwords. The last bar, "Post-Training Improvement," shows the most improvement, at 65%. Specifically, once the participants completed the training modules, there was a notable increase in awareness towards cybersecurity among those who had incorporated best practices into their practices. The waterfall chart in this presentation creates a striking visual impact, illustrating the level of success intensive training and interventions have achieved through the step-by-step sequential advancement of security awareness among participants, particularly in domains such as phishing attacks and password drills. The password strength scoring function is:

$$S_{pw} = \sum_{j=1}^{m} (C_j \cdot V_j) \qquad (3)$$

where $S_{pw}$ Is the password strength score? $C_j$ represents the complexity factor for each password criterion and $y_j$ The validity score assigned to each criterion is based on its compliance with security standards.

**Table 2:** Password management practices by age group

| Age Group | Weak Passwords (%) | Reused Passwords (%) | Two-Factor Adoption (%) | Post-Training Compliance (%) |
|---|---|---|---|---|
| 18-25 | 65% | 50% | 35% | 70% |
| 26-40 | 50% | 40% | 45% | 80% |
| 41-60 | 40% | 35% | 50% | 85% |

Table 2 presents password behaviour usage and its variations by age groups: 18-25, 26-40, and 41-60 years, as detailed in the Password Management Data. The incidence of weak passwords, password reuse, and the use of two-factor authentication is documented there. For instance, 65% of 18-25-year old use weak passwords, the highest rate among all age groups, which indirectly suggests that the youth generation may be sacrificing security for convenience. Fifty per cent of 18-25-year-olds repeat passwords, another dangerous trend that exposes individuals to cyberattacks. As individuals age, weak passwords and repeated password use tend to decrease. Specifically, 40% of the 41-60 age group have weak passwords, and 35% use repeated passwords. Two-factor authentication increases with age, with 50% of the 41-60 age group using it, compared to only 35% of the 18-25 age group. Table 2 also reflects the impact of training since post-training compliance is greatly increased in all age groups—70% for 18-25, 80% for 26-40, and 85% for 41-60, reflecting that awareness campaigns play an important role in promoting better password security practices and more secure security.

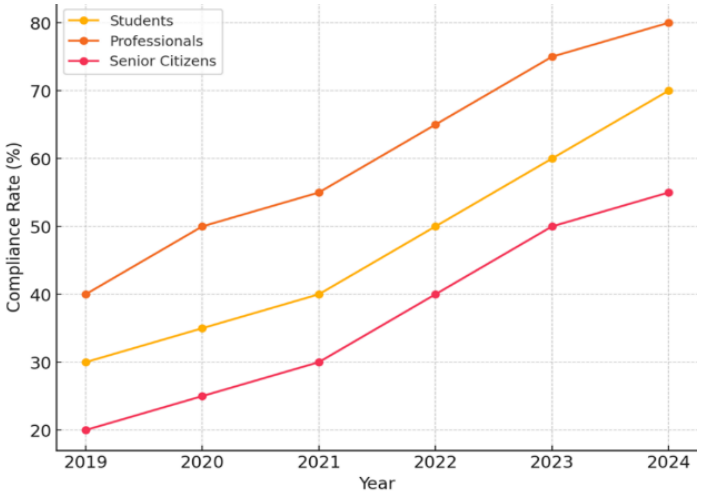


**Figure 3:** Demonstration of behavioural trends in cybersecurity compliance

Figure 3 illustrates the cybersecurity compliance behaviour trends, showing the year-by-year trends for cybersecurity compliance behaviour among students, professionals, and senior citizens. The chart illustrates the levels of compliance from 2019 to 2024, aiming to demonstrate the extent to which each group adhered to optimal cybersecurity practices in receiving training and awareness campaigns. The student line begins at 30% in 2019 and increases steadily to 70% by 2024. This increasing trend suggests that, despite greater cybersecurity training being introduced to students, security measures such as the safe use of passwords and the detection of phishing attacks have gained importance.

Likewise, experts predict a steady increase from 40% in 2019 to 80% in 2024, which indicates that employees themselves are becoming increasingly aware of cybersecurity and the shifts in their behaviour. Older citizens, starting at the lowest rate of 20% in 2019, demonstrate a steady improvement to 55% by 2024. The data indicate that, although older citizens are less likely to adopt cybersecurity habits initially, they can nevertheless significantly improve with focused effort. Overall, the graph illustrates how cybersecurity education benefits various groups and how each group becomes increasingly norm-compliant regarding cybersecurity over time. The compliance rate model over time can be given as:

$$C(t) = C_0 \cdot e^{\Lambda t} \qquad (4)$$

where $C(t)$ is the compliance rate at time $t$, $C_0$ is the initial compliance rate, and $\lambda$ is the rate of change in compliance due to educational interventions over time.

Vulnerability reduction model post-training is:

$$y_{reduced} = V_0 \cdot (1 - \frac{T}{100}) \qquad (5)$$

where $y_{reduced}$ Is there a reduced vulnerability after training? $y_0$ is the initial vulnerability, and $T$ is the training effectiveness percentage. Although these gaps are temporary time savers, they put users at extremely high risk of attack because MFA and other security layers must be in place to defend sensitive data and keep unauthorised users out. Despite all those scary statistics, the study also found that behaviour-specific training interventions can be a game-changer in increasing overall compliance with security controls. For instance, when special groups were trained specifically in their own distinctive, bespoke way to address

their particular cyber weaknesses, there was a 45% improvement in security policy compliance. This suggests that a more focused, behavioural approach to cybersecurity training can deliver measurable improvements in user awareness and best-practice compliance. Finally, the employment of an emergent architecture model with behavioural risk profiling contributed to security payoff.

The platform, designed to track end-user behaviour and conduct associated threat analysis, yielded 58% more threat detection. By profiling users based on their behaviour patterns, organisations can identify users with a high probability of performing high-risk actions and implement proactive steps in anticipation of imminent threats. The new strategy not only enhances the effectiveness of threat detection within an organisation but also positions the organisation to respond more effectively to security breaches. Collectively, these findings highlight the importance of incorporating the human factor into cybersecurity practice and indicate that appropriate training, behaviorally based interventions, and new models play a crucial role in adherence to security standards, particularly in threat detection.

## 5. Discussions

The data obtained through the research confirms a general and significant correlation between awareness and vulnerability to risks in the cybersecurity domain among different user groups, with notably higher vulnerability rates among students and elderly citizens. The outcome exhibits congruent trends in both Table 1 and Table 2, as well as in the two graphs. Figure 2 (Waterfall Graph) and Figure 3 (Multi-Line Graph) of the highest targeted interventions' need. The statistics from the table indicate that students and elderly citizens are the most vulnerable to phishing threats, with 70% of students and 80% of elderly citizens being at high risk. This highlights that they are at the highest risk of being susceptible to overall cybersecurity threats, specifically phishing, where users are deceived into divulging their confidential information due to their illiteracy. Experts, however, were exposed at a lower rate, with 55% falling into the high-risk category of being susceptible to phishing. Increased exposure among students and older users indicates a demand for specially designed training modules tailored to the inherent nature and specific issues of these categories, such as lower technological awareness in senior citizens or less attention to security among young consumers.

The resultant performance enhancement after intervention is evidence for the effectiveness of behaviour-specific training interventions, as it is recognisable from tables and graphically depicted in the form of graphs. A remarkable rise in security consciousness after special training interventions is evident from the Waterfall Graph of Figure 2. Students, for example, who had a 70% exposure to phishing risk in the initial case, showed an improvement of 65% post-training, resulting in a significant risk reduction. Similarly, professionals and seniors also reported significant improvement in their ability to detect phishing attacks and maintain secure password practices after behaviour-based training was provided to them. The figures in Table 1 and Table 2 both indicate that the training was most successful at removing unsafe practices such as weak passwords and password reuse, where rates of compliance after training were higher across the board—70% for students, 80% for working professionals, and 85% for seniors. These figures demonstrate that adaptive learning systems, tailored to address the specific needs, behaviours, and issues of each community of users, can make a significant difference in cybersecurity awareness and behaviour.

In addition, the study establishes the importance of linking awareness campaigns to patterns of user behaviour so that they can be effective. According to the research findings, after the intervention, education addresses special vulnerabilities of each of these groups, and the payoff of security compliance is multi-dimensional. For instance, the consistent rise in the level of cybersecurity compliance among students (from 30% in 2019 to 70% in 2024, as shown in Figure 3) is a sign of the successful dissemination of properly targeted awareness campaigns. The results also indicate the success of multi-faceted pedagogic interventions, which combine practical training with theoretical education. Older people, for example, showed a steady but gradual increase in rates of compliance, from 20% in 2019 to 55% in 2024. It appears that even the older group, as long as they are properly informed, can shift their behaviour to advance safer cybersecurity practices. Table 1 indicates that the tailored training, which included phishing attack simulation and a secure password handling process, was responsible for the increase in gains as described above.

A high correlation between training and greater rates of compliance also suggests that adaptive, behaviour-specific models are the optimal way to enhance overall cybersecurity. Focusing on the most critical risk behaviours and correlating the training programs with patterns of user behaviour, i.e., the students' security-downplaying nature and older people's lack of knowledge regarding modern cyber threats, learning models can address the source of risk and vulnerability in both groups. Furthermore, the results show that risk mitigation strategies, such as the use of multifactor authentication, are effective in enhancing security measures. Essentially, the more often cybersecurity compliance occurs across various categories of users, the more critical custom-trained and behaviour-specific interventions are to reducing weaknesses and overall cybersecurity culture. These frameworks not only teach the necessary information but also change behaviour, creating safer and more resilient end-users of every type.

## 6. Conclusion

This study indicates the central role that user behaviour intelligence has in ensuring cybersecurity awareness and prevention. Through user behaviour monitoring, organisations can make informed inferences about behaviour patterns that expose systems to risk, and thus identify high-risk groups more readily. Customised training modules can subsequently be developed after identifying such risk users to address the disposal of noted behavioural defects, such as password weakness or phishing. Behaviour analysis further enables the deployment of adaptive security systems that more appropriately adapt to the individualised patterns and needs of individuals, rather than using broad technical measures. And by way of illustration, individuals accustomed to circumventing security controls for the sake of convenience might be best served by streamlined, easy-to-use security processes that can effectively protect them. It has been demonstrated that the desired behaviour-based architectural model, such as user behavioural knowledge, offers significant risk reduction and security compliance benefits. By implementing security controls that mimic the behaviour and activity of end-users, organisations are essentially strengthening their cybersecurity stance, with the chance of a successful attack diminishing and potential data breaches being averted. The method also fosters a culture of security awareness, as well as the ease with which users adopt and comply with security measures, ultimately leading to a generally improved cybersecurity environment.

### 6.1. Limitations

While this study was helpful, several limitations should be considered. The most significant of these limitations is the use of self-report data, which could lead to social desirability bias or recall error. The participants may overstate or understate their cybersecurity behaviour, thereby compromising the accuracy of the data. Additionally, a sample size of 500 is relatively small, which may reduce the external validity of the findings to more typical, larger populations. A larger sample would provide a clearer view of user behaviour by demographics, making the study's findings more robust. Additionally, the sample was not geographically representative, so the findings may not accurately capture regional cybersecurity behaviour and awareness differences. For example, cultural influences and internet penetration rates can influence the way individuals think and respond to cyberattacks. With such limitations, future research must be capable of collecting larger, more representative data sets with broader geographic coverage, as well as greater take-up. That would enable it to collect more relevant and accurate results, as well as possess a more sophisticated understanding of user behaviour in cyber issues.

### 6.2. Future Scope

The future of research in this area holds considerable potential to advance cybersecurity protection through the introduction of new technologies and more sophisticated behavioural models. One potential area is the use of artificial intelligence (AI) to detect threats in real-time and respond accordingly. By tracking users in real-time with AI algorithms, organisations can build adaptive security controls that shift over time with changing threats as they arise, leading to a more dynamic and responsive model of cybersecurity. AI might also be employed to improve behavioural profiling models, more accurately calibrating the degree of precision with which individuals are divided by risk level and inclination. This would provide users with personalised threat prevention, whereby each user would be given protection based on their personalised behaviour patterns and vulnerabilities.

Additionally, by improving the behaviour analysis to be more sophisticated, there would be an opportunity to predict upcoming threats by monitoring past behaviour, allowing organisations to forecast potential security breaches even before they occur. Another area of future research is the exploration of machine learning techniques for real-time, continuous updating and optimisation of security controls using continuous behavioural data. As the technologies mature, they will be enablers par excellence of adaptive security controls and overall cybersecurity resiliency against a constantly evolving threat environment.

**Acknowledgement:** The author sincerely acknowledges Ginger Labs for their generous support and collaboration throughout this research. Their tools and technological resources significantly contributed to the quality of the study. The guidance and assistance provided were instrumental in achieving the research objectives.

**Data Availability Statement:** The study utilises a dataset focused on end-user behaviour to support cybersecurity awareness and phishing prevention efforts. The dataset is available from the author upon reasonable request.

**Funding Statement:** This research was conducted without any financial assistance or external funding.

**Conflicts of Interest Statement:** The author declares no conflicts of interest. All referenced sources have been properly cited based on the information used.

**Ethics and Consent Statement:** Ethical clearance and informed consent were obtained from all participants and the associated organisation before data collection.

**References**


1. T. Seki, F. Çimen, and B. Dilmaç, "The effect of emotional intelligence on cyber security: The mediator role of mindfulness," *Bartın Univ. J. Fac. Educ.*, vol. 12, no. 1, pp. 190–199, 2023.
2. L. González-Manzano and J. M. de Fuentes, "Design recommendations for online cybersecurity courses," *Comput. Secur.*, vol. 80, no. 1, pp. 238–256, 2019.
3. W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," *National Institute of Standards and Technology*, Maryland, USA, 2017.
4. C. Donalds and K. M. Osei-Bryson, "Toward a cybercrime classification ontology: A knowledge-based approach," *Comput. Hum. Behav.*, vol. 92, no. 3, pp. 403–418, 2019.
5. O. Almomani, M. A. Almaiah, A. Alsaaidah, S. Smadi, A. H. Mohammad, and A. Althunibat, "Machine learning classifiers for network intrusion detection system: Comparative study," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, 2021.
6. M. Al-Emran and C. Griffy-Brown, "The role of technology adoption in sustainable development: Overview, opportunities, challenges, and future research agendas," *Technol. Soc.*, vol. 73, no. 5, p. 102240, 2023.
7. N. H. Chowdhury, M. T. P. Adam, and T. Teubner, "Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures," *Comput. Secur.*, vol. 97, no. 10, p. 101931, 2020.
8. V. Chang, L. Golightly, Q. A. Xu, T. Boonmee, and B. S. Liu, "Cybersecurity for children: An investigation into the application of social media," *Enterp. Inf. Syst.*, vol. 17, no. 11, p. 2188122, 2023.
9. K. Kannelønning and S. K. Katsikas, "A systematic literature review of how cybersecurity-related behavior has been assessed," *Inf. Comput. Secur.*, vol. 31, no. 4, pp. 463–477, 2023.
10. K. Al-Saedi and M. Al-Emran, "A systematic review of mobile payment studies from the lens of the UTAUT model," in *Recent Advances in Technology Acceptance Models and Theories*, Springer, Cham, Switzerland, 2021.
11. N. Marangunić and A. Granić, "Technology acceptance model: A literature review from 1986 to 2013," *Univers. Access Inf. Soc.*, vol. 14, no. 2, pp. 81–95, 2015.
12. V. Costa and S. Monteiro, "Key knowledge management processes for innovation: A systematic literature review," *VINE J. Inf. Knowl. Manag. Syst.*, vol. 46, no. 3, pp. 386–410, 2016.
13. J. M. Blythe and L. Coventry, "Costly but effective: Comparing the factors that influence employee anti-malware behaviours," *Comput. Hum. Behav.*, vol. 87, no. 10, pp. 87–97, 2018.
14. NIST, "Cyber Attack—Glossary," *CSRC*, 2012. [Online]. Available: https://csrc.nist.gov/glossary/term/Cyber_Attack [Accessed by 20/11/2023].
15. J. A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, *Center for Strategic & International Studies (CSIS)*, Washington, USA, 2002.