Uniwersytet Jana Długosza w Częstochowie

Edukacyjna Analiza Transakcyjna 2025, nr 14

https://doi.org/10.16926/eat.2025.14.08

Zbigniew ŁĘSKI
https://orcid.org/0000-0003-4145-6955
Jan Długosz University in Częstochowa
e-mail: zleski@ujd.edu.pl

Passivity in Transactional Analysis and the Susceptibility of Users to Cyber Threats

How to cite [jak cytować]: Łęski, Z. (2025). Passivity in Transactional Analysis and the Susceptibility of Users to Cyber Threats. *Edukacyjna Analiza Transakcyjna*, *14*, 139–148.

Abstract

This study investigates the relationship between passivity strategies in transactional analysis and users' susceptibility to cyber threats. The main research problem concerned identifying which passive strategies are most strongly associated with risky online behaviours. The study was conducted in Poland using the CAWI method on a sample of 357 adults. Two tools were employed: the Passivity Questionnaire (Pierzchała, 2024) and the author's experimental Cyberthreat Susceptibility Questionnaire (Łęski, 2024). The results revealed statistically significant correlations between the strategies of Overadaptation and Doing Nothing and susceptibility to cyber threats, partially confirming the hypothesis that all forms of passivity increase risk. A positive relationship was also found between the Violence strategy and displaying one's private life on social media, which may indicate reduced sensitivity to privacy and a link to sharenting. These findings highlight the importance of psychological factors in cybersecurity and may inform preventive and educational initiatives aimed at strengthening users' digital self-protection competences.

Keywords: transactional analysis, passive strategies, cybersecurity, susceptibility to digital threats

Introduction

Cybersecurity is currently one of the key and most frequently discussed areas of research. It encompasses not only technical issues related to the security of hardware and software, but also social and personality aspects. Ultimately, it is the human being – the user of information systems – who determines whether the implemented protective mechanisms prove effective or not. Maalem Lahcen et al. (2020) point out that most cybersecurity incidents stem from the human factor. Effective protection therefore requires an interdisciplinary approach, integrating knowledge from computer science, psychology, criminology, and the behavioural sciences.

Recent studies have confirmed that human factors significantly impact cybersecurity, and that a holistic approach considering human behaviour and performance is crucial for both achieving and maintaining security principles (Al-Badayneh et al., 2025). Similarly, Nikum (2025) emphasises that attackers deliberately exploit psychological traits such as trust, curiosity, or cognitive shortcuts to gain unauthorised access through social engineering techniques like *pretexting*. This demonstrates that cybersecurity is not only a technological issue but also a deeply psychological and behavioural challenge. Wiederhold (2014) likewise argues that incorporating psychological insights addressing phenomena, such as bounded rationality and optimism bias, can substantially improve decision-making and reduce susceptibility to cybercrime.

In this context, it is particularly important to address the behavioural and social aspects of cybersecurity. As Kennison and Chan-Tin (2020) emphasise, in addition to users’ knowledge and skills, their risk-taking tendencies and personality traits should also be taken into account. The authors suggest that such an approach can account for as much as 34% of the variance in engaging in risky online behaviours. Significant predictors of susceptibility to online threats also include internet addiction and impulsivity (Hadlington, 2017). In contrast, Łęski (2024) found a positive correlation between susceptibility to cyber threats and the tendency to enter negative affective states, as well as a negative correlation with orientation towards positive states.

These findings indicate that prevention in the field of cybersecurity should involve not only the transfer of knowledge about technical safeguards but also concern for the mental and emotional well-being of users. Concepts that enable a clear and accessible description of complex mechanisms of human behaviour are particularly useful here. One such framework is transactional analysis, which meets these conditions and makes it possible to interpret susceptibility to cyber threats in terms understandable to a broad audience.

Passivity in Transactional Analysis

In this article, susceptibility to cyber threats is analysed in relation to the phenomenon of passivity, defined within the framework of transactional analysis. Passivity does not merely denote a lack of action, as it is commonly understood, but also encompasses behavioural strategies that fail to lead to constructive problem-solving. According to the *Lexicon of Transactional Analysis Concepts and Terms*, passivity is defined as 'a failure to take responsibility for one's thinking, actions, and feelings. It is characterised by doing nothing or acting ineffectively, while at the same time withholding information about oneself. Passive behavioural strategies indicate the presence of discounting (ignoring information) and, through manipulation, compel another person or the wider environment to resolve one's problems' (Jagieła, 2023).

Five basic strategies of passivity are distinguished:

- **Doing Nothing:** directing energy towards refraining from action rather than addressing the problem.
- **Overadaptation:** excessive conformity to the expectations of others.
- **Agitation:** expending energy on repetitive, purposeless actions.
- **Incapacitation:** presenting oneself as incapable of acting and shifting responsibility onto others.
- **Violence:** expressing frustration through aggression towards the environment.

In the context of cybersecurity, each of these strategies may constitute a significant risk factor. Doing Nothing encourages neglect of basic security principles, such as using strong passwords or updating software. Overadaptation may lead to behaviours that conform to group expectations but fail to address individual risks. Agitation manifests as thoughtless, repetitive online actions, increasing the likelihood of incidents. Incapacitation may result in relinquishing responsibility for one's own digital security, and, when combined with Violence, can also involve behaviours that jeopardise the safety of other users.

In summary, the passivity strategies described in transactional analysis can serve as useful predictors of susceptibility to cyber threats, underscoring the need to consider psychological factors more fully in digital security research.

An important point of reference in the study of passivity is the work of A. Pierzchała, who addresses the issue from both a practical and a scholarly perspective. Her research explores, among other aspects, the phenomenon of passivity in the school environment, revealing its significant prevalence among both students and teachers (Pierzchała, 2013). In the context of this study, this is particularly relevant: if the hypothesis of a positive correlation between passive behaviours and susceptibility to cyber threats is confirmed, then a high level of passivity in schools – Institutions intended to foster attitudes conducive to cybersecurity – must be regarded as a serious concern.

In her work, Pierzchała does not confine herself to identifying the phenomenon of passivity but also investigates its sources and potential protective factors. In one of her projects, she demonstrated that a high level of emotional intelligence shields individuals from the destructive manifestations of passivity. In the same publication, she also examined *reflectivity*, analysed through the dimensions of lack of self-confidence and caution. The results suggest that lack of self-confidence reinforces passivity in all its aspects, whereas caution functions as a protective factor (Pierzchała, 2024). Pierzchała's findings show that passivity is a complex phenomenon, the intensity of which depends both on risk factors and on the resources available to the individual. These conclusions affirm the value of exploring the relationship between passivity and susceptibility to cyber threats.

Methodological Assumptions

The aim of this study was to examine potential correlations between users' tendencies to apply specific passive strategies and their engagement in behaviors that may compromise cybersecurity. The research was conducted in Poland using the CAWI (Computer-Assisted Web Interviewing) method on a sample of 357 adults.

The group comprised 276 women and 81 men. The respondents' ages ranged from 18 to 76 years, with a mean age of 27.6 years for women and 31.6 years for men (median age: 23 in both groups). Most participants assessed their own competence in using new technologies as average, which suggests a relatively typical level of digital literacy among Internet users.

The central research question was formulated as follows: *Are there statistically significant correlations between individual passive strategies and users' tendencies to engage in risky online behaviors and to disregard basic cybersecurity principles?*

Accordingly, the following hypothesis was proposed: *There are statistically significant correlations between each of the passive strategies and the propensity to engage in potentially dangerous online behaviors.*

Two research instruments were employed. The first was the Passivity Questionnaire (PQ), developed by A. Pierzchała. This tool has undergone validation procedures and is scheduled for publication in the *Przegląd Badań Edukacyjnych* (*Polish Journal of Educational Research*) in 2025. It was previously used by Pierzchała (2024) to investigate the relationship between passivity, emotional intelligence, and reflectiveness.

The second instrument was the Cyberthreat Susceptibility Questionnaire (CSQ), developed by the author. It consists of 16 items addressing potentially risky online behaviors and adherence to basic cybersecurity principles. The questionnaire can be analyzed at both the item level and as a single scale measuring susceptibility to cyber threats. The Cronbach's alpha coefficient was approximately 0.7, which, given the exploratory character of the instrument, indicates acceptable reliability. This tool has already been used in the author's earlier research on relationships between ego states in transactional analysis, affective tendencies, and susceptibility to cyber threats (Łęski, 2024).

Similar diagnostic tools have been developed in other countries, including the Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al., 2017) and the Visual Analogue Scales (VAS) for modelling cyber-secure behaviour (Raywood-Burke et al., 2021). These instruments demonstrate that psychological and behavioural dimensions of cybersecurity can be measured reliably. However, they are typically designed for corporate or institutional environments, focusing on employees' compliance with organisational security policies. In contrast, the CSQ was designed to capture broader psychosocial aspects of cybersecurity relevant to ordinary Internet users, including personality-related and emotional factors described within the framework of transactional analysis. Thus, the tool extends the existing research tradition by addressing cybersecurity as a human–psychological phenomenon, not merely a technological or procedural one.

It is important to acknowledge certain limitations of the research. Conducting the survey online may have favoured individuals already comfortable with technology, potentially less susceptible to digital threats. Moreover, the gender imbalance in the sample, with women constituting nearly 77% of participants, may influence the generalisability of the findings. Future studies should therefore strive for a more balanced sample and include variables such as the intensity and context of Internet use, which could moderate the relationships between passivity strategies and susceptibility to cyber threats.

The study was conducted in Polish. For the purposes of this publication, the results and instruments were translated into English. It should be noted, however, that no validation studies have yet been conducted for English-language versions of the tools.

Research Results

Due to the specific characteristics of the study group, Spearman's non-parametric correlation was used to identify potential relationships between variables. A summary of the correlations between the five passive strategies and statements from the Cyberthreat Susceptibility Questionnaire, where the coefficients were statistically significant, is presented in Table 1.

Table 1

Correlations between passive strategies and behaviors potentially affecting cybersecurity. Statistically significant correlations are indicated in bold and with an asterisk.

	Passive Strategies:				
Cybersecurity:	**Violence**	**Incapacitation**	**Agitation**	**Overadaptation**	**Doing Nothing**
I am able to effectively search for and select information on the Internet.	0.083	-0.062	0.051	**-0.167***	0.035
I like to use the Internet late in the evening or at night – that's when I have peace and no one bothers me.	0.030	0.096	0.093	0.090	**0.204***
In my online relationships, I sometimes react with anger and aggression.	0.050	**0.174***	0.033	**0.166***	0.091
Inviting people I've never met in real life to my circle of friends/followers on social media is OK.	0.035	-0.006	0.020	0.029	**0.107***
I try to use strong passwords, containing combinations of different characters, and different ones for each important service I use.	-0.079	-0.041	0.004	**-0.120***	0.013
On social media, I like to show my friends what I'm doing, where I'm going, what I'm watching, etc.	**0.106***	0.053	0.017	0.013	-0.050
If I encounter violence on the Internet, I don't do anything – reacting in this environment is pointless.	-0.102	-0.056	-0.061	0.022	**0.155***
Sometimes I visit sites with content like sex or violence – everything is for people.	-0.073	0.024	-0.102	0.027	**0.125***

Source: Author's own research.

The statistical analysis revealed no strong associations. It should be emphasized that the Cyberthreat Susceptibility Questionnaire used in this study is an experimental tool that requires further refinement and validation. Nevertheless, the analysis of statistically significant correlations allowed the identification of noteworthy tendencies. Among the examined strategies, Doing Nothing and Overadaptation displayed the highest number of significant associations with risky behaviors. No statistically significant results were obtained for the Agitation strategy.

The Doing Nothing strategy was positively correlated with the statements:

— 'I like to use the Internet late in the evening or at night—that's when I have peace and no one bothers me.'

— 'Inviting people, I've never met in real life to my circle of friends/followers on social media is OK.'

— 'If I encounter violence on the Internet, I don't do anything—reacting in this environment is pointless.'

— 'Sometimes I visit sites with content such as sex or violence—everything is for people.'

These results suggest a user profile characterized by a passive and conformist attitude. Such individuals may opt for solutions that demand minimal cognitive and emotional effort (e.g., not verifying the identity of people on social media, not reacting to violence). Preference for nighttime activity may reflect a search for comfort, while accessing potentially harmful content may stem from its easy availability and its role as an accessible outlet for negative emotions.

The Overadaptation strategy was negatively correlated with declared competencies in searching for and selecting information and in using strong passwords. At the same time, it was positively correlated with a tendency to react with anger and aggression in online interactions. The negative correlations with digital competencies raise important questions. Do they reflect actual deficits, or rather low self-esteem and lack of confidence, consistent with the construct of Overadaptation? This issue requires further investigation, preferably with objective measures of competence. At the same time, the positive correlation with online aggression suggests that over-adaptive individuals may use cyberspace as an outlet for negative emotions. While in direct interactions they may suppress their needs to meet the expectations of others, the anonymity of online settings can facilitate the expression of frustration, consequently leading to risky behaviors.

A positive correlation was also found between the Incapacitation strategy and the propensity for anger and aggression online. Similar to individuals using the Overadaptation strategy, this may suggest that helplessness or passivity in the offline world is compensated for by aggressive behavior in the digital environment.

An interesting result was observed for the Violence strategy, which showed a positive correlation with the statement: *"On social media, I like to show my friends what I'm doing, where I'm going, what I'm watching, etc."* At first glance, this connection is not obvious. However, interpretation should be approached with caution. It can be assumed that both phenomena are underpinned by a need to demonstrate control and influence over the environment, as well as a limited respect for others' boundaries. In this context, it is worth referring to the increasingly debated phenomenon of "sharenting" (parents publishing images of their children), which some researchers classify as a form of digital violence that infringes on a child's privacy and autonomy. Nevertheless, this relationship requires in-depth analysis in future research.

When the analysis was conducted not at the level of single statements, but on the entire Cyberthreat Susceptibility scale, only one statistically significant correlation coefficient was observed for the Overadaptation strategy. Prior research by Pierzchała (2013) indicates that Overadaptation is among the most frequently observed passive strategies. The present results show that reliance on this strategy significantly increases cybersecurity risks, as confirmed by both the overall scale and item-level analysis. Over-adaptive individuals, seeking above all to conform to external demands, may neglect issues important from their own perspective, including those related to digital security.

Summary and Conclusions

The purpose of the research presented in this publication was to determine potential correlations between users' tendency to employ specific passive strategies and their susceptibility to cyber threats. The main risk profiles identified are related to the strategies of Overadaptation and Doing Nothing, which displayed the highest number of significant correlations with risky online behaviours. Therefore, the hypothesis proposed in the methodological section was only partially confirmed.

The Overadaptation strategy was the only one that also showed a significant relationship with the overall scale of susceptibility to cyber threats, suggesting its dominant role as a potential risk factor. The results indicate that individuals who rely on this strategy may be less confident in their digital skills and more prone to compliance with external demands, which can reduce their attention to personal online safety. Similarly, the Doing Nothing strategy reflects a tendency to avoid effort or responsibility, which may indirectly increase exposure to online risks.

Some relationships, such as the correlation between aggressive tendencies and self-disclosure on social media, should be treated as hypothetical interpretations rather than confirmed empirical findings. While they may point to a reduced sensitivity to privacy or phenomena like *sharenting*, such assumptions require further verification.

The results obtained here are partly consistent with international research highlighting the role of human factors in cybersecurity (e.g. Hadlington, 2017; Parsons et al., 2017; Wiederhold, 2014; Al-Badayneh et al., 2025; Nikum, 2025), which confirm that psychological traits and behavioural patterns significantly influence vulnerability to digital threats. By applying the framework of transactional analysis, this study extends that perspective, emphasising the relevance of passivity as a psychological correlate of cyber-risk exposure.

It is important to note several limitations of the study. The online form of data collection may have favoured participants already familiar with digital technologies, while the gender imbalance (77% women) limits the generalisability of the findings. Moreover, the Cyberthreat Susceptibility Questionnaire used in this research is still in its experimental stage, and the results should be interpreted as exploratory.

Future studies should include more balanced and cross-cultural samples, and combine self-report data with behavioural indicators of cybersecurity practices. Such research would help determine whether the observed relationships are context-specific or universal, and contribute to the development of comprehensive psychological models of user susceptibility to digital threats.

References

Al-Badayneh, D., Al-Badayneh, D., & Hashish, R. (2025). Human Factors of Cybersecurity. *Journal of Posthumanism*. https://doi.org/10.63332/joph.v5i4.1242.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Jagieła, J. (2023). *Leksykon pojęć i terminów analizy transakcyjnej*. Wydawnictwo Naukowe Uniwersytetu Jana Długosza w Częstochowie.

Kennison, S., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviours. *Frontiers in Psychology, 11*, 546546. https://doi.org/10.3389/fpsyg.2020.546546

Lahcen, R., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioural aspects of cybersecurity. *Cybersecurity, 3*, 1–16. https://doi.org/10.1186/s42400-020-00050-w

Łęski, Z. (2024). The profile of ego states and experiencing positive and negative feelings in the context of vulnerability to cyber threats. *Edukacyjna Analiza Transakcyjna, 13*, 137–152. https://doi.org/10.16926/eat.2024.13.08

Nikum, A. (2025). Examining the Human Factors in Cybersecurity Practices: Psychological, Technical, and Organisational Perspectives. *Asian Journal of Research in Computer Science*. https://doi.org/10.9734/ajrcos/2025/v18i6699.

Pierzchała, A. (2013). *Pasywność w szkole*. Wydawnictwo AJD w Częstochowie.

Pierzchała, A. (2024). Emotional intelligence and reflexivity vs. passivity in the perspective of transactional analysis: A research report. *Edukacyjna Analiza Transakcyjna, 13*, 189–202. https://doi.org/10.16926/eat.2024.13.11

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Comput. Secur.*, 66, 40-51. https://doi.org/10.1016/j.cose.2017.01.004.

Raywood-Burke, G., Bishop, L.M., Asquith, P.M., Morgan, P.L. (2021). Human Individual Difference Predictors in Cyber-Security: Exploring an Alternative Scale Method and Data Resolution to Modelling Cyber Secure Behavior. In: Moallem, A. (eds) *HCI for Cybersecurity, Privacy and Trust. HCII 2021. Lecture Notes in Computer Science()*, vol 12788. Springer, Cham. https://doi.org/10.1007/978-3-030-77392-2_15

Wiederhold, B. (2014). The Role of Psychology in Enhancing Cybersecurity. *Cyberpsychology, behavior and social networking*, 17 3, 131-2 . https://doi.org/10.1089/cyber.2014.1502.

Pasywność w ujęciu analizy transakcyjnej a podatność użytkowników na cyberzagrożenia

Streszczenie

Badanie dotyczy związku pomiędzy strategiami pasywności w analizie transakcyjnej a podatnością użytkowników na zagrożenia cybernetyczne. Główny problem badawczy koncentrował się na identyfikacji tych strategii pasywności, które najsilniej wiążą się z ryzykownymi zachowaniami w sieci. Badanie przeprowadzono w Polsce metodą CAWI na próbie 357 osób dorosłych. Zastosowano dwa narzędzia badawcze: Kwestionariusz Pasywności oraz autorski, eksperymentalny Kwestionariusz Podatności na Cyberzagrożenia. Wyniki ujawniły istotne statystycznie korelacje pomiędzy strategiami nadadaptacji i bierności a podatnością na zagrożenia cyfrowe, co częściowo potwierdza hipotezę, że wszystkie formy pasywności zwiększają ryzyko. Dodatkowo odnotowano dodatni związek pomiędzy strategią agresji a ujawnianiem życia prywatnego w mediach społecznościowych, co może wskazywać na obniżoną wrażliwość na prywatność i związek ze zjawiskiem sharentingu. Uzyskane wyniki podkreślają znaczenie czynników psychologicznych w cyberbezpieczeństwie i mogą stanowić podstawę dla działań profilaktycznych oraz edukacyjnych ukierunkowanych na wzmacnianie kompetencji użytkowników w zakresie ochrony cyfrowej.

Słowa kluczowe: analiza transakcyjna, strategie pasywne, cyberbezpieczeństwo, podatność na zagrożenia cyfrowe.