Human Factors in Social Engineering: Psychological Components and Profiling of Targets

Andreea BURADA
Bucharest University of Economic Studies, Romania
buradaandreea20@stud.ase.ro

This paper examines the psychological underpinnings of human susceptibility to social engineering, with a focus on identifying and analysing the cognitive, emotional, and behavioural components that contribute to target vulnerability. Integrating insights from cybersecurity studies and psychological theory, this research seeks to construct a nuanced understanding of how threat actors manipulate human factors to bypass security protocols. Through critical analysis of empirical studies, documented attack scenarios, and profiling literature, the study aims to determine the strongest factors that influence one's susceptibility to becoming a victim, as well as understand the process behind a threat actor. The paper defines multiple categories of users that are deeply correlated to social engineering attacks and aims to establish an early methodology of determining one's typology.
Keywords: *Cybersecurity, Social engineering, Psychology, User typologies*
DOI: 10.24818/issn14531305/29.4.2025.02

1 Introduction

The most prevalent component that is daily exploited by malicious individuals is not the computer, as many would be inclined to believe, but the human. While firewalls, encryption algorithms, and security protocols protect the machines, the human mind remains deeply vulnerable, posing a constant and continuously evolving risk. As technology evolved, the focus on security measures shifted to systems, architectures, protocols, and other elements of this nature, whereas the anthropoid component received less attention.

The cross-field of psychology and social engineering is not fully investigated. [1] There is more room for scientific pursuit of the topic; different approaches are required to build the full picture of the issue. In particular, the need for interdisciplinary research becomes apparent with the real implications of social engineering attacks. Previously, frameworks have been established, but they rely heavily on technical measures, which prove to be insufficient when the vector of attacks is cognitive manipulation, which bypasses typical cybersecurity countermeasures. The comprehension of people's acts before and during a social engineering attack, regardless of type, is the pinnacle of achieving a system that can withstand such attacks.

Herein lies the importance of examining psychological profiling: the attacker's chances of success are greatly increased by their capacity to collect behavioural data, predict reactions, and customise interactions to an individual's personality. This work is crucial not only for prevention but also for the development of more nuanced educational tools. Cybersecurity awareness training often treats users as uniform recipients of static information, rather than as diverse individuals influenced by personality traits, emotional states, and cognitive limitations. By integrating psychological insights, such programs can be made more effective, personalised, and engaging. Elevating the human factor from a liability to a locus of resilience is both a challenge and a necessity in the evolving digital threat landscape.

The aim of the paper is to establish multiple goals and attempt to find answers or directions that provide some clarity into the subject. The following empirical questions have been determined as the primary focus of the thesis:

- What types of users can be identified?
- What is characteristic of each type?
- Are certain social engineering attacks linked to one or more types?

Once the foundation of typologies has been established, the objectives of the paper can be highlighted and the results analysed. Primarily, the focus is to identify said classification and define each in depth. The ability to determine a person's digital personality as a combination of indexes of all the typologies represents the most complex challenge of this research.

2 Literature Review

2.1 Introduction to Social Engineering

As technology rapidly advances, newer and more complex attacks are attempted by hackers in everyday scenarios. Systems become more convoluted with the aim of preventing breaches and malware, but the most important component, the human, remains overlooked. As previously stated, the research of the psychological component in the sphere of social engineering, although it exists, is limited and scarce. Thus, it is imperative to take a different approach in regard to cybersecurity and gradually introduce concepts of psychology and human nature.

2.2 Classic Classification of Attacks

Before any categories of character can be defined, it is crucial to note the different types of social engineering that are generally regarded as standard [2]:

Phishing is the act of committing cybercrime through the action vector of a falsified e-mail with the appearance of legitimate content. The goal is gaining access to sensitive knowledge, such as banking details, passwords, or identifiable information. [3]

Phishing is the most popular attack method used to gain secret information from users; an estimated 3.4 billion spam emails are sent every day attempting to fraudulently gain access to users' accounts. [4] Financially, the consequences are dire, with significant losses for companies that suffer data breaches as a result of successful phishing attacks. The cost of such an attack against an organisation is, on average, more than 4 million dollars.

Due to the substantial number of attacks of this type, multiple subcategories have been defined based on the targeted victims as well as the hackers' goals. "*Spear phishing"*, as the name suggests, is a focused approach to phishing, attempting to retrieve sensitive data of a specific individual, group, or organisation [5]. Additionally, defined by their distribution channel types, "*vishing"* and "*smishing"* are terms often heard and recognised by cybersecurity enthusiasts. In the modern era, most people own smartphones and are frequently utilising them, creating an opportunity for attackers to exploit this channel of communication. With the advancement in artificial intelligence models, hackers have developed methods to mimic the voices of loved ones or authorities that create a genuine impression of urgency or trust for the victims.

Albeit similar to phishing, *pretexting* represents a more sophisticated and targeted form of social engineering. It relies heavily on inciting the feeling of familiarity when interacting with the victim, which psychologically triggers an increase in trust. [6] As a hacking vector, pretexting is surprisingly effective, taking advantage of human traits, such as the ability to trust, low perception of threat, and susceptibility to react based on emotions in different scenarios. [7]

With the advancement of technology, hackers can perform these attacks with ease over the phone or through messages, often spending longer periods of time building trust with the target until eventually, unbeknownst to them, they become victims of financial loss.

Akin to pretexting, ***baiting*** is a type of social engineering attack that convinces the victim, using trust techniques and manipulation, to perform a risky action or divulge confidential information. The attackers take advantage of certain psychological phenomena, like curiosity and greed, to influence the victim in a certain aspect. [8] There are two categories of baiting: using digital bait or physical bait. Both are effective for different scenarios or groups of individuals, the former more popular for attacks that occur across country borders or at long distances, whereas the latter

is particularly preferred when the location of the victims is known and can be accessed easily.

A ***quid pro quo*** attack is a type of social engineering tactic where a cybercriminal promises a victim a benefit in exchange for sensitive information. The phrase "quid pro quo" comes from Latin and means "something for something" [9], and it encompasses the essence of the attack. People are deceived into performing unsafe actions or divulging secret information because of the false sense of trustworthiness triggered by the premise of a promise.

With the identification and awareness of the loneliness epidemic that the youth is struggling with, the need for socialisation has shifted from in-person interaction to digital exchanges. It is significantly easier for many users to talk to people online, as they can have a better appearance through their online persona. This type of attack is called ***honey trap,*** and it specifically targets this category of people. This trick involves the criminal pretending to be an attractive person online. The person befriends their targets and fakes an online relationship with them. The criminal then takes advantage of this relationship to extract their victims' personal details, borrow money from them, or make them install malware into their computers.

Rogue security software might appear in the form of rogue anti-malware, rogue scanners, rogue scareware, anti-spyware, and so on. This type of computer malware misleads users into paying for simulated or fake software that promises to remove malware. Rogue security software has become a growing concern in recent years. An unsuspecting user might easily fall prey to such software, which is available in plenty.

It is important to remember that in most scenarios multiple social engineering attacks are combined to achieve results. Human nature can be easily exploited if the attacker has a deep understanding of psychology, behavioural tendencies, patterns of actions, etc.

2.3 Introduction to Victimology

A great discipline of interest and inspiration is victimology, the branch of criminology that studies the relationship between a victim and an offender by focusing on the causes and consequences of the incident. This speciality focuses greatly on the injured party's state of mind prior to and following the crime, with analysis of the factors that led to the misdemeanour and identification of elements that could have prevented the incident.

Previous research identified multidimensional victim typology frameworks but has not established categories of victims. Landau and Freeman-Longo, in "*Classifying Victims: a Proposed Multidimensional Victimological Typology*" [10], a notorious study of the 90s in this field, proposed eleven dimensions to their framework that act as guidelines to defining typologies but does not propose any categories itself. In modern literature, many topics of discussion are focused on the perpetrators, and they attempt to explain the mentality that determines someone to cause harm to another person.

3 Methodology of Cyber-Victimology

In the previous chapters, the importance of psychology in the domain of cybersecurity has been established. The lack of research that intertwines the two fields of study has formed a gap of knowledge in terms of defining, designing, and maintaining a defence system.

3.1 User Typologies

Whilst the field of cybersecurity does not include a strong knowledge of psychology, certain definitions, concepts, perspectives, and approaches can be adapted to encompass a methodology that combines the two disciplines and allows for the discovery of better methods of analysis and protecting victims of cybercrime. In the article "*Victimology from clinical psychology perspective: psychological assessment of victims and professionals working with victims*" [11], the author argues that personality is a relevant psychological factor when considering the effects of victimisation. Thus, nine categories of users with respect to

both digital and psychological behaviours have been defined in this paper. Each classification has certain types of social engineering attacks that portray the belonging people as targets at a higher risk. It is important to note that a user's conformation is comprised of all categories in different proportions.

The Opportunist

The "*opportunist"* is defined as the user who puts their goals above the means of attaining them, wanting so fervently to obtain something that they are willing to risk their own digital safety. Most commonly, this category includes the individuals who seek to acquire content, like music, movies, or video games, through illegal sources, which are heavily populated with adware and malicious pop-ups. This group may be aware of the risks of engaging with untrustworthy web pages, yet they accept the potential consequences for the chance of obtaining their goal.

The "*opportunist*" typology is not limited to pirated content only; it extends to any digital user behaviour that includes a predefined goal and the resistance to accepting that the goal cannot be attained. Their lack of security through prevention oftentimes leads to clicking on malicious links or downloading viruses. From a cybersecurity perspective, this category is most susceptible to attacks of the type of malware obtained from dubious sources, adware, malicious pop-ups, and cross-site scripting. The "*opportunist"* is desperate in their attempts to obtain what they seek and behaves gullibly.

Table 1. Proposed questionnaire for "Opportunist" typology

Question	Answer	Score*
Can digital piracy be ethical under certain conditions?	Yes.	0.25
	No.	-0.4
When you are overly excited about a video game/movie/TV show, do you feel that you cannot wait to enjoy that media?	Yes, I cannot wait.	0.1
	No, I can wait for it to be released publicly.	-0.2
Would you consider yourself a person who gives up easily?	Yes.	-0.3
	No.	0.2
"I trust online communities when they deem a source as safe"	True	0.15
	False	-0.05
When you find something online that you were searching for for a long time, you …	Check if there are reviews or opinions from other users about the source.	-0.2
	Regardless of feedback, you try your luck by downloading the content.	0.35
"I have great confidence in my ability to find anything online"	True	0.1
	False	-0.2
"I am not afraid to run executables acquired from the internet, knowing they might be a free version of the software I want"	True	0.65
	False	-0.3

The Digital Drifter

The term *"digital drifter"* alludes to the concept of a speck of dust drifting in the wind; likewise, some users navigate the web with little to no attention directed at the content they interact with. To some extent, all individuals exhibit this behaviour in different ratios or at different times, but this category differentiates itself from the typical relaxed Internet activity by having the user predominately act in this manner, rarely manifesting an elevated attentiveness level. This type of individual is oftentimes nonchalant and easy-going, using the Internet primarily to relax or wind down after a day of work.

As a matter of fact, the concept of "autopilot" behaviour is exceedingly relevant to the "*digital drifter"* typology since this concept is the quintessence of the category. The majority of users act on autopilot, but digital drifters do it the majority of the time. Exhaustion and overstimulation can cause an individual to engage in activities like mindlessly scrolling social media platforms or random web pages. This occurrence has been studied in recent years with the popularisation of platforms like TikTok and content like Instagram Reels, YouTube Shorts, etc. The reason behind the success of this phenomenon is rooted in psychology, as viewing content of this type triggers the release of dopamine, a neurotransmitter that is linked to happiness, pleasure, excitement, and satisfaction of rewards [12]. Additionally, there is a slight overlap with the "*tech-averse*" typology, as people with a disinterest in technology are prone to not be careful when visiting websites and clicking on different images, links, or advertisements.

Despite the crossover, a person with a high technical comprehension can exhibit periods of time in which they act according to this typology.

Table 2. Proposed questionnaire for "Digital Drifter" typology

Question	Answer	Score*
Do you often spend countless hours scrolling mindlessly on your device?	Yes.	0.4
	No.	-0.1
"I usually use the Internet to relax in my free time."	True	0.1
	False	-0.3
"When I use social media I ..."	Only check my notifications and messages.	-0.15
	Endless scroll for hours to relax.	0.25
Have you ever noticed you were not fully attentive and in the moment when browsing the Internet?	Yes.	0.2
	No.	-0.4
Do you feel that social media has negatively impacted your attention span?	Yes.	0.05
	No.	-0.05
"Most times when I use the Internet I ..."	Act on instinct, not thinking much about what I am doing.	0.45
	Search for something.	-0.35
"I consider myself just a casual digital user."	True	0.3
	False	-0.15

The Loner

The "*loner*" is a particularly interesting typology; isolated from friends and relatives, they seek social interaction online, believing it is easier to attain it digitally. They refrain from interacting with others in real life out of a fear of rejection. These people oftentimes are loyal members of different communities, like online forums. There are two important dynamics that are identified regarding the "*loner*" type: the cause and the consequence. The latter is similar to what has been described previously, where the scarce social life of a person determines an increased digital usage, whereas the former refers to individuals who spend so much time online that it negatively impacts their life. The general behaviour of the "*loner*" can be associated with that of an addicted person. A study from 2022 [13] analysed the prevalence of Internet addiction and its negative effects, finding that addiction to digital content can exacerbate anxiety and depression.

In cybersecurity, "*loners*" become the perfect targets due to their desperation for human connection and naivety towards potential dangers. Whilst genuine relationships can form online, many romantic interactions are simply attempts of hackers to manipulate unsuspecting victims into believing that by providing financial benefits, the victim will receive amorous fulfilment. The issue is so widespread that banks, card companies, and governments have officially issued warnings about "romance scams", or as others call them, "honey trap" attacks.

Table 3. Proposed questionnaire for "Loner" typology

Question	Answer	Score*
"I find it easier to talk to people online than in real life."	True.	0.2
	False.	-0.3
"When a person wants to befriend me online I ..."	Am cautious about their intentions.	-0.35
	Reciprocate with excitement.	0.25
Do you consider internet friends to be real friends?	Yes.	0.3
	No.	-0.4
Do you find yourself often spending more time online than offline?	Yes.	0.4
	No.	-0.45
Do you consider yourself at least somewhat addicted to using the Internet?	Yes.	0.35
	No.	-0.3
Online relations are just as important as offline relations.	True.	0.2
	False.	-0.35

The Tech-Averse

The individuals that are considered to belong to the "*tech-averse"* typology have a general disinterest in learning about technology, knowing enough to utilise devices or the internet to obtain the information or perform the action they need to, but nothing beyond that point. The term "digital literacy" refers to one's ability to use a digital device or medium correctly, efficiently, and safely. An International Computer and Information Literacy Study (ICILS) [14] conducted in 2023 found that 43% of students do not hold a basic level of digital skills. Previously this study was done in 2018, and 6 years later, most countries have a downward or stagnant tendency. From a behavioural perspective, the "*tech-averse*" individual is able to complete digital tasks despite the lack of in-depth knowledge. Websites, applications, and even forums have evolved to have user-friendly designs and functionalities so as to encourage

people with a reduced digital literacy to use their product.

From a cybersecurity standpoint, users who have a limited understanding of technology are easier to convince of untruths, such as that clicking on a certain link can guarantee a prize or various unrealistic scenarios with the pretext of obtaining money. Untrained individuals, like the "*tech-averse*" person who has little to no knowledge about the workings of the digital world, represent the majority of the victims of phishing attacks [15]. Social engineering attacks of the type "*quid pro quo*" can also be efficient against this typology.

Table 4. Proposed questionnaire for "Tech-Averse" typology

Question	Answer	Score*
"I do not see the need to know much about technology"	True	0.3
	False	-0.25
Do you understand most of the programs that you use?	No, I just know the few things I need to do.	0.25
	Yes, I understand it well.	-0.4
"Technology is over my head and it frustrates me."	True	0.35
	False	-0.25
"Learning about some of the latest tech trends is entertraining."	True	-0.5
	False	0.1
"When I have to use a digital tool that I do not know I ..."	Get frustrated and discouraged.	0.4
	Search for tutorials and manage to use it fairly easy.	-0.35
"Using something without understanding it is wrong."	True	-0.3
	False	0.15

The Fringe Believer

This typology encompasses people who belong to controversial communities, named by some "echo chambers", in which they support one another's unconventional beliefs. These individuals, known as conspiracy theorists, have built digital circles where they can meet like-minded people with whom they engage. The behaviour of a "*fringe believer*" is driven by the feeling of isolation due to a different mindset and the feeling of being misunderstood. The Internet has made various theories very popular, like the belief that the Earth is flat or that the moon landing was fake. Some are harmless, whilst others are controversial and cruel; conspiracy theories divide people, with many people not continuing to stay friends with those of drastically opposite mindsets. A study [16] done on school pupils reveals that 52% of the students would not stay friends with someone who believed in a particular conspiracy theory they deemed delusional and unbelievable.

Additionally, the security aspect of this typology is interesting, as "*fringe believers*" become victims of common social engineering attacks as well but targeted to their beliefs. In reality, hackers understand the subtleties of this typology and build payloads that can convince a bigger group of people who fall under a similar conspiracy to click on a malicious link or download a suspicious file.

Table 5. Proposed questionnaire for "Fringe Believer" typology

Question	Answer	Score*
"When I see a new conspiracy theory online I ..."	Take interest quickly.	0.2
	Keep scrolling, it's nonsense.	-0.3
"I have one or multiple beliefs that others consider delusional, but others online agree with me."	True	0.3
	False	-0.25
Are you the type of person to primarily base your opinions on facts and proof?	Yes.	-0.2
	No.	0.15
"I believe in things that cannot be proven if others come up with a convincing theory."	True	0.25
	False	-0.3
Do you doubt most things that you see online?	Yes.	-0.35
	No.	0.15
"I found a community online that believes in a conspiracy theory. My first reaction is ..."	To question if they do not have better things to do.	-0.4
	To read about their theory and maybe start believing in it too.	0.35
"A friend posted about a crazy theory that they came up with. I ..."	Message them to remove the post to not embarrass themselves.	-0.35
	Ask more information about the theory.	0.2

The Skeptic

As previous chapters focused on the unknowing or reserved digital users, it is important to recognise that there are many people who are very careful when entering the digital world. Some exhibit overbearing levels of caution, being paranoid that any online interaction can lead to a virus or infection with malware. This individual is identified and defined in this paper as the "*skeptic*", the person who takes all the precaution measures to not become the victim of a hacker and who uses the Internet

with "silk gloves". Contrary to popular belief, the "*skeptic*"'s routines and safety methods are not impenetrable; on the contrary, their tendencies to navigate the Internet with fear create ample opportunities for hackers to devise specialised methods that target this category. This typology does not target specific individuals of a certain background; anyone can ultimately develop a strong fear of cybersecurity attacks, considered by many a valid concern with the increasing number of incidents. Moreover, as one learns more about the dangers of the digital world, they might develop tendencies belonging to this typology that were not present prior.

The most efficient type of social engineering attack, perhaps, is the rogue security attack in which a "*skeptic*" is convinced that their computer has been compromised. A calm and calculated person, despite the threat, knows that they have security measures in place and will use those instead. Additionally, ransomware attacks pose a good method to exploit the nature of these users, as they entice fear and panic.

Table 6. Proposed questionnaire for "Skeptic" typology

Question	Answer	Score*
Do you frequently clear your cookies as to avoid websites tracking you?	Yes	0.3
	No	-0.2
"I often double-check a link before I click on it."	True	0.25
	False	-0.3
"If I clicked on something suspicious by accident, I immediately get nervous and overthink."	True	0.4
	False	-0.25
Do you consider yourself moderately to highly afraid of infecting your device with malware?	Yes.	0.35
	No.	-0.3
Are you deeply concerned with security and privacy matters on the Internet?	Yes, the safer I am the better I feel.	0.4
	No, I am not that concerned about my online safety.	-0.3
"I am reluctant to run any executibles from the Internet."	Yes, even those from safe sources.	0.35
	No, only if there is a reason to be suspicious.	-0.2
Have you ever acted opposite to your character in a state of high panic?	Yes, when I am scared I am emotional.	0.35
	No, even when scared I can be rational.	-0.25

The People-Pleaser

The "*people-pleaser*" is a bit peculiar in the sense that they seek to help others as much as they can and receive personal satisfaction when doing so. Psychologically, some core principles of this mindset are avoiding conflicts of all types, defining self-worth and self-esteem based on the approval of others, trying to influence the thoughts of others, and instilling a positive image of oneself through helpful acts [17]. However, despite the positive outside appearance, this behaviour is detrimental to the actor, as they often fail to set healthy boundaries with others. The individuals in this typology have a tendency to aggregate in communities in which their help is sought after and their need for validation is exacerbated. Putting their needs above others, they find ways to prioritise the other party to complete the request they have received. Thus, the vicious circle continues, the "*people-pleaser*" seeking the next "target" to help and realising too late that they have spent too many hours into the night helping strangers that they will never talk to again.

Naïve and willing to believe in the best outcome, the "*people-pleaser*" will not need a lot of convincing to consider a pretexting attack as true. Their need to help others overcomes rationale. Moreover, quid pro quo attacks are particularly successful since the individual of this category feels less pressure to perform an act due to the reciprocity. The "*people-pleaser*"'s lack of clear boundaries and fear of being impolite also create great opportunities for attackers to perform physical social engineering attacks. It is significantly easier to tailgate someone who will avoid emphasising the misconduct due to avoiding causing a conflict or raising tension between the two parties.

Table 7. Proposed questionnaire for "People-Pleaser" typology

Question	Answer	Score*
"I really enjoy giving advice online to others."	True	0.15
	False	-0.2
Have you ever helped someone online to your detriment? (stayed	Yes	0.3
	No	-0.25

awake later, postponed doing something etc.)		
"I have difficulty saying no to people even when it is inconvenient to me."	True	0.3
	False	-0.25
Do you feel personal validation when you help others?	Yes	0.25
	No	-0.3
"I am part of one or more online communities where the main goal is to help others."	True	0.2
	False	-0.4
"When I think that I may have upset someone, I..."	Feel very bad about it and try to make amends ASAP.	0.45
	Evaluate the situation to see if their reaction is valid.	-0.3
"The way others see me is very important to me."	True	0.3
	False	-0.35

The Thrill Seeker

Some people seek intense experiences when they browse the internet, hence the typology name "*thrill seeker*". These individuals prefer to frequent lesser-known areas of the World Wide Web. As their interests are not mundane, "*thrill seekers*" frequent the deep web or the dark web, either to browse for fun or to survey what interesting content is available. Contrary to popular belief, the deep web is the biggest part of the web, but it is not indexed and is not as easily accessible. The deep web is seemingly innocent, comprising unsearchable data storages for support services, banks, or companies [18]. The "*thrill-seeker*" finds excitement in browsing this part of the Internet, as it requires more skill than the average user possesses to get access.

Anyone can exhibit behaviours belonging to this typology, regardless of morality or technical knowledge, as the biggest influencer is the component of curiosity. These users also demonstrate a level of impulsiveness influenced by their desire for stimulating content. However, their impulsivity often causes them to become victims of various cybersecurity attacks, like adware that is found on the deep or dark web due to the decreased level of security, viruses from files obtained in this area of the Internet, and even some forms of phishing.

Table 8. Proposed questionnaire for "Thrill Seeker" typology

Question	Answer	Score*
"When I see a video on my feed with a content warning I ..."	Click on it out of curiosity.	0.2
	Scroll, it might distress me.	-0.3
Have you ever accessed the dark web out of curiosity?	Yes.	0.25
	No.	-0.35
Do you often seek out new and intense experiences even if they make you nervous?	Yes.	0.35
	No.	-0.3
Have you ever intentionally visited a website that might expose you to emotionally distressing content? (eg: the 50/50 website)	Yes.	0.4
	No.	-0.3
"I often get bored when browsing the Internet if I do the same thing over and over again."	True	0.25
	False	-0.2
"I willingly expose myself to content that others might be shocked by." (true crime, NSFL content, etc.)	Yes.	0.45
	No.	-0.4
Would you be willing to perform grey-area activities for the thrill of it?	Yes, I don't have much remorse regarding it.	0.4
	No, I don't want to risk doing anything illegal.	-0.35

The Ethical Purist

A more difficult category to define, the "*ethical purist*" is a person with a very high sense of morality, with a need to respect the law and regulations constantly, and who sometimes holds others accountable for their behaviour online. These individuals consider laws and rules to be the most important thing and are very rarely influenced to disregard their moral code. The "*ethical purist*" can even be perceived as unbearable by others because they have no issue disregarding the feelings of others to let morality and order rule their interactions and actions. Through a psychological filter, these individuals can show a lower level of empathy to their peers as they consider righteousness to be the most important element. They recognise the importance of feelings and subjectivity, but, regardless, they consider rules to be of utmost importance.

However, despite the immediate appearance that this category is predominantly positive, there are certain drawbacks to be considered. Hackers, for instance, are aware of this personality type, and they construct targeted whaling or spear phishing campaigns that are significantly successful. They recognise the behavioural patterns that make the "*ethical purist*" use their rationality over emotions and use this feature to their advantage.

Table 9. Proposed questionnaire for "Ethical Purist" typology

Question	Answer	Score*
Do you think it's wrong to break the rules, even if doing so might lead to a better outcome?	Yes, rules are made to always be followed.	0.35
	No, sometimes it is needed to break the rules.	-0.3
Do you avoid using software, services, or platforms if you know they exploit users or violate privacy even though you need to use them?	Yes.	0.4
	No.	-0.3
Have you ever taken a stand against a group decision because you felt it violated core ethical principles?	Yes	0.3
	No	-0.25
"I think feelings can be a weakness."	True	0.2
	False	-0.25
"If one of my friends does something illegal, I will probably …"	Report them to authorities, it is the right thing to do.	0.4
	Talk to them about it and see if we can find a solution.	-0.3
Would you unfriend someone over moral conflicts?	Yes.	0.25
	No.	-0.35
If a rule/law would endanger someone's wellbeing (physical or mental), would you follow the rule regardless?	Yes.	0.45
	No.	-0.25

3.2 Tabulation Method for Digital Personality Constructs

To collect the data, a questionnaire containing the questions mentioned in the previous tables has been distributed in the form of a website. For computing the result of the questionnaire per typology, each answer has a score attributed, which represents the weight of the influence the answer has over the result. These scores have been chosen arbitrarily based on the research conducted for each typology and prior knowledge of psychological and cybersecurity elements.

Thus, a normalised simple formula has been identified that is used to calculate the score for each typology based on the results received as follows:

$$S_T = (S_{obtained} - S_{min})/(S_{max} - S_{min}) \cdot 100,$$

where S_T represents the score of a typology, $S_{obtained}$ is the score calculated based on the answers of a user, and S_{min} and S_{max} are computed using the negative scores (S_{min}) and positive scores (S_{max}).

As stated prior, the construct of a user's cyber-personality is comprised of all typologies with their respective scores. Relationships between types will be analysed based on the sample collected. Additionally, accuracy of the methodology will increase as more questions are defined and added to the pool, creating more variability between possible user results and a more significant reflection of one's digital activity.

4 Results

The relevancy of the study is primarily determined through the analysis of the results collected. Despite the reduced number of responses, there is insight to be gained from the current research.

The survey, at the time of writing this paper, has been completed by 66 users, with a gender distribution of 50% (33 participants) being female, 40.9% (27 participants) being male, and the rest either non-binary or undisclosed.

The age demographic shows a strong preference of people under 30 years old to complete the quiz, with 45.5% (30 participants) in the age group "25-34 years" and 31.8% (21 participants) in the "18-24 years" age group. The dominant environment of the responders is the urban area, with 50 of the total number of participants (75.8%) belonging to urban environments. In terms of education, the highest occurrence is the master's degree, representing 33.3% of the responses. Accumulatively, the percentage of participants who have at least a bachelor's degree is 74.2%, indicating a well-educated sample of participants. The employment status is majorly "employed full-time" (66.7%). However, there are participants of all other types of employment, including retirement.

For each typology, the mean score of the percentages obtained for all responses has been calculate, as it can be seen in **Fig. 1**. The "*opportunist*" has a mean of 56.27%, representing the highest mean across all typologies, and around 60% of the users had at least a medium risk level in this category. The second highest is marked by the "*digital drifter*" with a mean

of 56.09%, indicating that the overall risk level of the public is relatively high. These findings are somewhat expected, as many people have a tendency of spending mindless time on their devices.

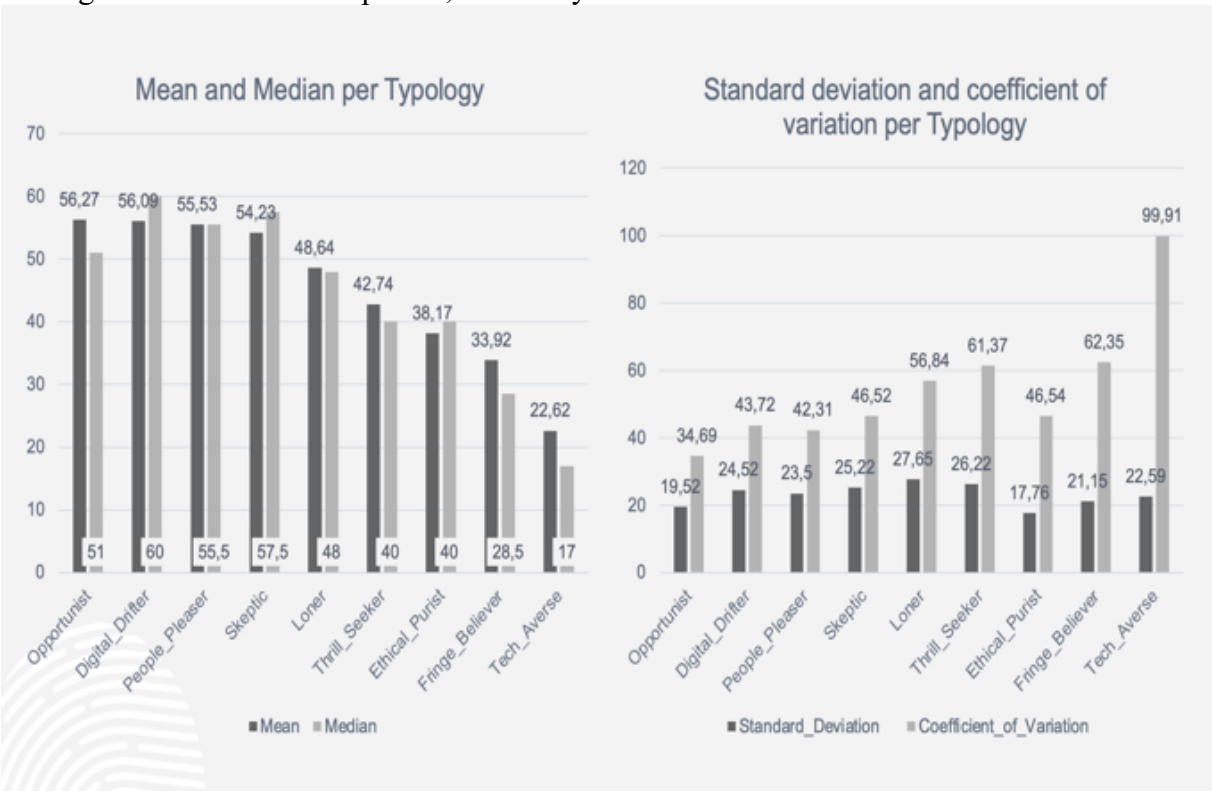

Fig. 1. Bar charts describing the mean, median, standard deviation, and coefficient of variation for each typology

With a mean of 55.53% based on the results collected as of now, the "*people pleaser*" has very similar average performances to the previous category. Interestingly, there is a moderate to strong correlation identified between the "*people pleaser*" and "*digital drifter*" (coefficient of 0.364). Marking a source of interest, the "*skeptic*" typology has a mean of 54.23%, relatively high, showing that a significant number of participants are concerned over their digital safety. The "*loner*" has a lower mean of 48.64%; additionally, the age group "18-24 years old" has a higher mean score for this category (55.43%), indicating that these users have a higher risk of isolation from others and the habit of retreating to the digital world for escapism. The "*thrill seeker*" typology analysis presents a bimodal distribution, with users most likely belonging to a very high-risk level or a very low-risk level. Men tend to partake in risky online activities related to the need for experiencing strong emotions, as the mean for the male participants is 31% higher than the mean of the female participants. The overall mean of this typology is 42.74%. The "*ethical purist* has a mean value of 38.17%. The "*fringe believer*" also possesses a low percentage of responders that classify as high-risk (only 6%) and has a mean of 33.92%. Lastly, the typology "*tech-averse*" has the lowest mean out of all the categories (22.62%), as most of the participants have careers or professional activities in the technology sector. This typology might be slightly biased; further analysis will be required.

5 Conclusions

In the ever-growing world of digital content, where technology continuously advances, the number of cyber threats continues to rise as well. As complex as already established solutions may have become, one critical element is omitted from the entire equation: the human. Recent studies have recognised the importance of focusing on the human element, as

the person behind the system represents the biggest security vulnerability. Thus, the gap in literature and research on this topic has been identified. Few papers or implementations focus on the cross between human nature and the digital world, between psychology and cybersecurity. It is of utmost importance to consider these two elements, as ignoring the psychological elements of the security problems will lead to the same issues that have been encountered previously.

This thesis proposes a new methodology of, currently, nine typologies of digital users, focusing strongly on the behaviour, intentions, tendencies, and habits of people when they interact with the digital world. The methodology attempts to profile a person by determining the typological components of their digital personality.

Following the distribution of a questionnaire, valuable data has been collected and analysed, and conclusions regarding the typologies proposed have been reached. The consensus is that there is relevancy to the typologies and questions. Multiple correlations have been established between typologies or between typology and demographic information.

References

[1] A. H. Washo, "An interdisciplinary view of social engineering: A call to action for research," Computers in Human Behavior Reports, vol. 4, 2021.

[2] "SentinelOne," 17 October 2024. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/types-of-social-engineering-attacks/. [Accessed 10 April 2025].

[3] "Phishing.org," [Online]. Available: https://www.phishing.org/what-is-phishing. [Accessed 10 April 2025].

[4] AAG IT Services, "AAG," [Online]. Available: https://aag-it.com/the-latest-phishing-statistics/. [Accessed April 2025].

[5] M. Kosinski, "What is spear phishing?," IBM, 6 June 2024. [Online]. Available: https://www.ibm.com/think/topics/spear-phishing. [Accessed April 2025].

[6] Zscaler, Inc., "What Is Pretexting?," Zscaler, Inc., [Online]. Available: https://www.zscaler.com/zpedia/what-is-pretexting. [Accessed May 2025].

[7] K. F. Steinmetz, "The Identification of a Model Victim for Social Engineering: A Qualitative Analysis," An International Journal of Evidence-based Research, Policy, and Practice, vol. 16, pp. 540-564, 2021.

[8] Light Reading Inc., "Social Engineering, the USB Way," Light Reading Inc., 2006.

[9] Nord VPN, "Quid Pro Quo Attack," [Online]. Available: https://nordvpn.com/cybersecurity/glossary/quid-pro-quo-attack/. [Accessed May 2025].

[10] S. F. Landau and R. E. Freeman-Longo, "Classifying Victims: a Proposed Multidimensional Victimological Typology," International Review of Victimology, vol. 1, no. 3, pp. 267-286, 1990.

[11] T. Yılmaz, "Victimology from clinical psychology perspective: psychological assessment of victims and professionals working with victims," Current Psychology, vol. 40, pp. 1592-1600, 2021.

[12] R. Chamat, "Why We Keep Scrolling: The Psychology of Infinite Feeds," 16 December 2024. [Online]. Available: https://ewm.swiss/en/blog/why-we-keep-scrolling-psychology-infinite-feeds [Accessed June 2025].

[13] R. Lozano-Blasco, A. Q. Robres and A. S. Sanchez, "Internet addiction in young adults: A meta-analysis and systematic review," Computers in Human Behavior, vol. 130, 2022.

[14] International Computer and Information Literacy Study, "ICILS 2023 International Report: An International Perspective on Digital Literacy," IEA, 2023.

[15] E. Mouncey and S. Ciobotaru, "Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness," Journal of Economic Criminology, vol. 7, 2025.

[16] BBC, "Conspiracy theories: What are the most popular and why do they spread?," February 2025. [Online]. Available:

https://www.bbc.co.uk/bitesize/articles/z2pbxg8. [Accessed June 2025].
[17] J. Sheffe, " Internal Motivations of People Pleasers," Sparrows Nest Counseling, 28 August 2024. [Online]. Available: https://www.sparrowsnestcounseling.com/blog/internal-motivations-people-pleasers. [Accessed June 2025].
[18] ID Agent, "Who Are Today's Dark Web Users?," 23 March 2023. [Online]. Available: https://www.idagent.com/blog/who-are-todays-dark-web-users/. [Accessed June 2025].
[19] L. Jaeger and A. Eckhardt, "Eyes wide open: The role of situational information security awareness for security-related behaviour," Information Systems Journal, vol. 31, no. 3, pp. 429-472, 2020.
[20] G. Wright, "DEFINITION dumpster diving," TechTarget, April 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/dumpster-diving. [Accessed May 2025].
[21] J. Hamzelou, "Your autopilot mode is real - now we know how the brain does it," New Scientist Ltd., 23 October 2017. [Online]. Available: https://www.newscientist.com/article/2151137-your-autopilot-mode-is-real-now-we-know-how-the-brain-does-it. [Accessed June 2025].

Andreea BURADA graduated from the Faculty of Cybernetics, Statistics, and Economic Informatics in 2023 with a bachelor's in economic informatics, having studied the courses in English. She continued her studies within the same faculty, graduating in 2025 with a master's diploma in cybersecurity. She is deeply passionate about psychology and strives to attain a career that combines her knowledge in the cybersecurity world and her deep desire to perform humanitarian work.