UDC 316.6:004.7

Andrii Shpilkin, student,
Kharkiv National University of Radio Electronics
andrii.shpilkin@nure.ua

PSYCHOLOGY OF CYBERSPACE. SOCIAL MEDIA ADVANTAGE FOR THREAT ACTORS

Abstract. *This work is dedicated to the study of the existing patterns in cybersecurity and their relation with overall trends in cyberpsychology. Also, the object of social media for phishing and analysing behaviour is covered.*

Cybersecurity is only establishing subject of computer science. However, with the rapid development of information communication technology, the importance of it is growing every year.

Even though a lot of advanced tools and techniques compromise a system, the most effective remains the same for a lot of years straight. Some organizations, such as Identity Defined Security Alliance (IDSA), have gathered data from more than 500 individuals, who are responsible for information technology (IT) or security departments and have more than 1000 employees [1]. The results of the questionnaire are shown in Figure 1.

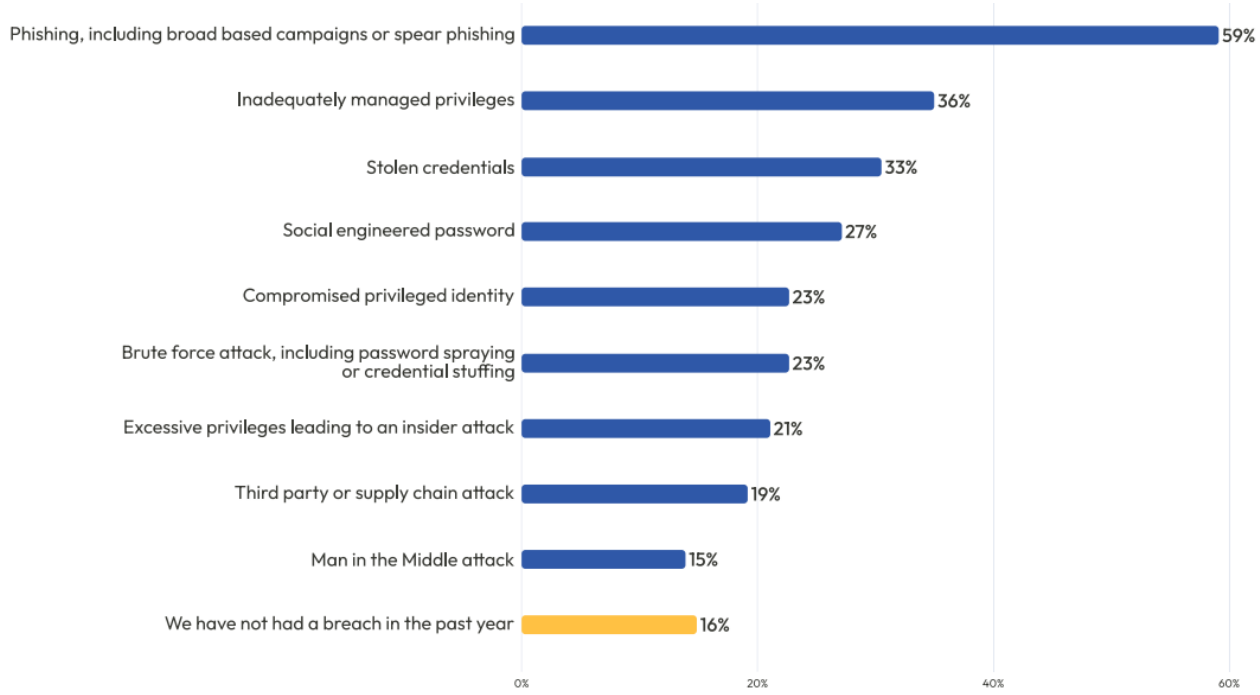

Figure 1 – Kinds of identity-related breaches in companies for 2021

By analysing Figure 1, it can be concluded that all kinds of phishing (spear phishing and others) remain the top threat for companies with a 59% rate. Socially engineered passwords have

occurred in 27% of organizations. The famous case of the Uber breach in the autumn of 2022 emphasizes the importance of staying cautious for not to become the next breached company or individual.

The interesting thing is that by adding insider attacks due to excessive privileges, the percentage of breaches related to humans significantly rises up. That is why people are the weakest link in cybersecurity.

And from that perspective, cyberpsychology started to form as an independent area, with a focus on understanding the psychological processes related to and underlying, all aspects and features of technologically interconnected human behaviour [2].

All our interactions on the Internet remain there. And the users form their digital footprint. By analysing comments and photos, the Big 5 personality traits can be predicted (Azucar et al. [3]). The Big 5 model is one of the most used in behavioural sciences. It consists of five dimensions – wide categories of personal traits.

Competence, self-discipline, self-control, perseverance and a sense of duty are all aspects of conscientiousness and adherence to rules and regulations.

Positive emotions, friendliness, assertiveness, ambition and a sense of adventure are all characteristics of Extraversion.

Compassion, cooperation, belief in the inherent goodness of people, reliability, helpfulness, obedience and directness are all characteristics associated with agreeableness.

Being open to new and different experiences, inventive ideas and unconventional views implies a tendency towards creativity, adaptability and imagination.

The tendency to experience negative emotions, anxiety, pessimism, impulsivity, susceptibility to stress and self-doubt are characteristics of neuroticism [4].

According to this information, a threat actor can try to use some of the six methods of influence that were represented by famous psychologist and academic R. Cialdini in his book «Influence».

Authority – this implies that people tend to obey the orders or requests from those, who are hierarchically higher by their position or status.

Commitment and consistency – mostly, the majority of people try to act consistently in similar situations.

Reciprocity – based on the social norms to give back after favour.

Liking – if one human likes another, it results in a higher agreement rate.

Social proof – as people try to seem normal and fit in society, they trust more to someone who has done such things before.

Scarcity – limitation of resources. This technique is widely used in marketing because rare things make people desire them more. Even information with limited access persuades better [4].

Figure 2 represents the relation between the Big 5 model and Cialdini's influence methods [4].

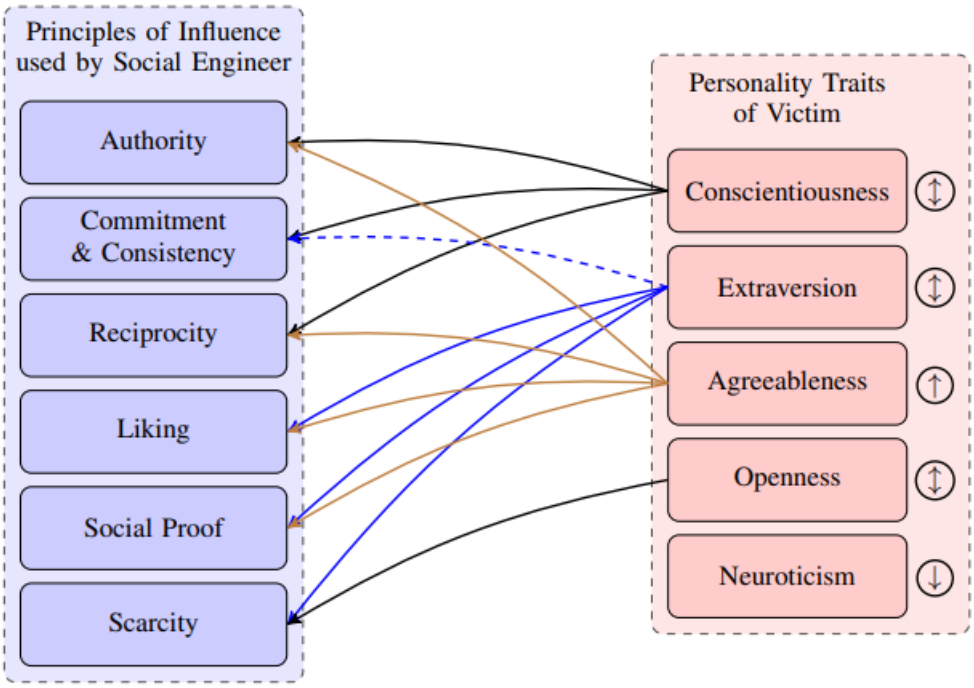

Figure 2 – The relation between the Big 5 model and Cialdini's influence methods

Analysis of Figure 2 also shows how personality traits affect susceptibility to phishing messages. Arrow up – for increasing this chance, down – for decreasing and two-way arrow – for both (depends on circumstances and not yet researched extensively).

So, because people can intentionally or unintentionally disclose a lot of personally identifiable information (PII), the task becomes much easier for threat actors. Of course, because threat actors often do not know their victim, they are more likely to use authority or urgency (lack of time).

Research by Alkhalil et al [5] also emphasizes that age and demographics are important factors to define the resistance of soshing (a term to refer phishing through social media). In general, young adults from 18 to 25 and old people (65+) click on the phishing link with more probability. Demographics here represent not only nationality but rather the working environment. For example, those who spend more time in front of computers are less susceptible to these threats. The same is true for information technology and engineering students.

The CERT-UA has documented cases of phishing attacks in Ukraine involving fraudulent SMS messages as well as fraudulent emails purporting to be official government communications. In one worrying incident, people are having 10 UAH deducted daily from their bank accounts as a result of unauthorised SMS subscriptions to unidentified services. These incidents highlight the need for people to be vigilant, to be cautious when disclosing personal information, and to use security measures to protect themselves against phishing scams and unauthorised financial transactions.

It is clear from the evidence presented that successful phishing attacks require not only technical expertise but also an understanding of human psychology. Phishers use psychological vulnerabilities including trust, curiosity, and the desire for rewards to trick others into falling for their frauds. As a result, it is critical to educate oneself on basic phishing strategies as well as the psychological manipulation involved.

A multi-pronged approach is required to effectively combat phishing efforts. Individuals might benefit from awareness training in recognizing and responding to phishing threats. Technical methods such as spam filters, encryption, and two-factor authentication can provide additional protection layers. Furthermore, legal measures are critical in pursuing and discouraging those who engage in phishing activities.

By combining knowledge of psychology with technical safeguards and legal action, individuals and organizations can enhance their defences against phishing attacks and protect themselves from the potential harm caused by online scams.

References:

1. 2022 Trends in Securing Digital Identities [Electronic resource] // Identity Defined Security Alliance. – [2022]. – Mode of access: https://assets.beyondtrust.com/assets/documents/2022-Trends-in-Securing-Digital-Identities.pdf
2. Cyberpsychology: Defining the Field [Electronic resource] // Psychology Today. – [2020]. – Mode of access: https://www.psychologytoday.com/us/blog/the-cyberpsychology-page/202011/cyberpsychology-defining-the-field
3. Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. Personality and Individual Differences [Electronic resource] // Azucar, Danny & Marengo, Davide & Settanni, Michele. – [2018]. – Mode of access: https://www.researchgate.net/publication/321965757_Predicting_the_Big_5_personality_traits_from_digital_footprints_on_social_media_A_meta-analysis
4. The Social Engineering Personality Framework [Electronic resource] // Uebelacker, Sven & Quiel, Susanne. – [2014]. – Mode of access: https://www.researchgate.net/publication/271135217_The_Social_Engineering_Personality_Framework
5. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy // Alkhalil Zainab & Hewage Chaminda & Nawaf Liqaa and Khan Imtiaz. – [2021] – Mode of access: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full