Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Human Factor in Cybersecurity: Behavioral Insights into Phishing and Social Engineering Attacks

Sudha Rani Pujari[1], Mahmood Afzal Hussain[2]
[1]*Independent Researcher, University of the Cumberlands*
[2]*Researcher, Department of Information Technology, University of the Cumberlands*

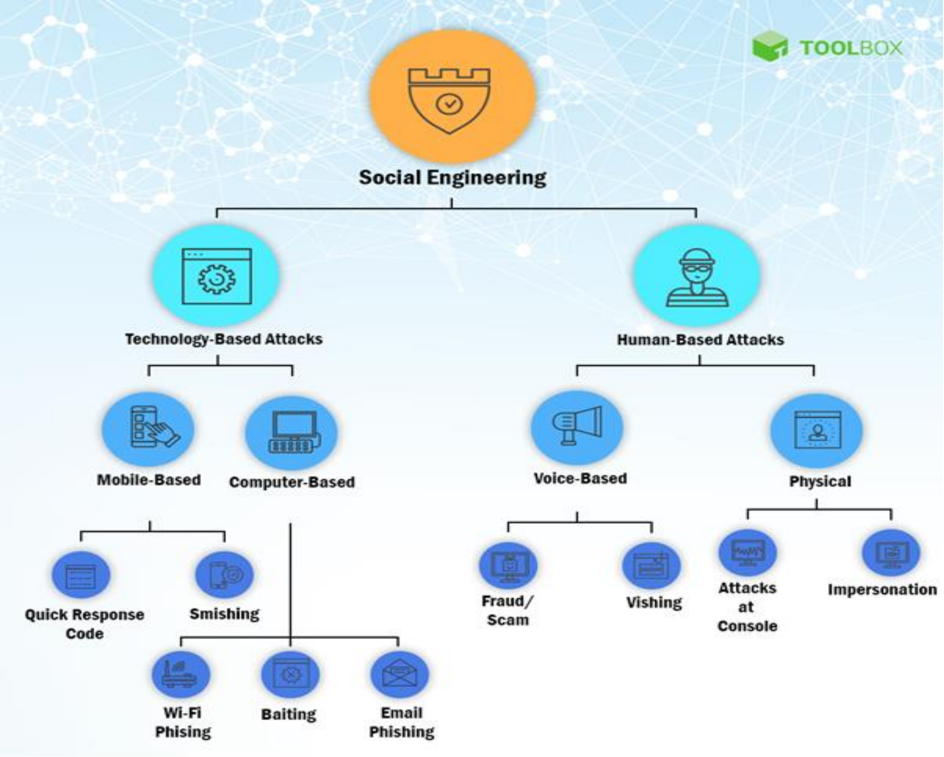
In this paper, we explore the role of human behavior in cybersecurity by looking at phishing and social engineering as an example. It will explore the role that psychological and behavioral factors play as vulnerabilities and what may be done to reduce the risk of human error. The methodology used in the study is a systematic review involving existing literature from empirical studies, case analysis, and theoretical frameworks. Part of this research integrates human factors in cybersecurity by integrating findings from psychology, information technology, and organizational behavior on human factors in cybersecurity. Results from the study demonstrate that phishing and social engineering succeed due to cognitive biases, low awareness, and lack of training. It also identifies effective countermeasures: Minimum susceptibility can be reduced through tailored training programs, behavioral nudges, and technical interventions. The research shows that behavioral insights have to be included in the cybersecurity strategy. This increases the organization's overall security posture across all systems, and the value comes from designing interventions to address human vulnerabilities. From a social perspective, the outcomes accentuate the need for broad training and identification battles in people and networks of people. In this study, we offer a novel, interdisciplinary view of human factors in cybersecurity. This book aims to connect the dots between behavioral science and cybersecurity practice, providing action-oriented findings to researchers, practitioners, and practitioners who want the human element out of cyber risk.

Keywords: Human factors, cybersecurity, phishing attacks, social engineering, behavioural insights, cognitive biases, cybersecurity awareness.

1. Introduction

Today, in the digital era, Cybersecurity is still a concern, especially in the fast-moving digital world. Despite a massive arms race of technological advancement to bolster our defences, human behaviour has proven to be almost the most exploited vulnerability by

Cybercriminals. The need for the human factor in Cybersecurity is shown by the phishing and social engineering attacks, which use the human factor, not a technical one. In this paper, I show how three behavioural dimensions of Cybersecurity—cognitive biases, decision-making process, and social dynamics—contribute to the effectiveness of phishing and social engineering. By looking back at existing literature and case studies, the study tries to identify patterns of human behaviour that make them vulnerable to these attacks. To help drive more effective means to increase cybersecurity awareness and resilience, these insights are valuable to know.

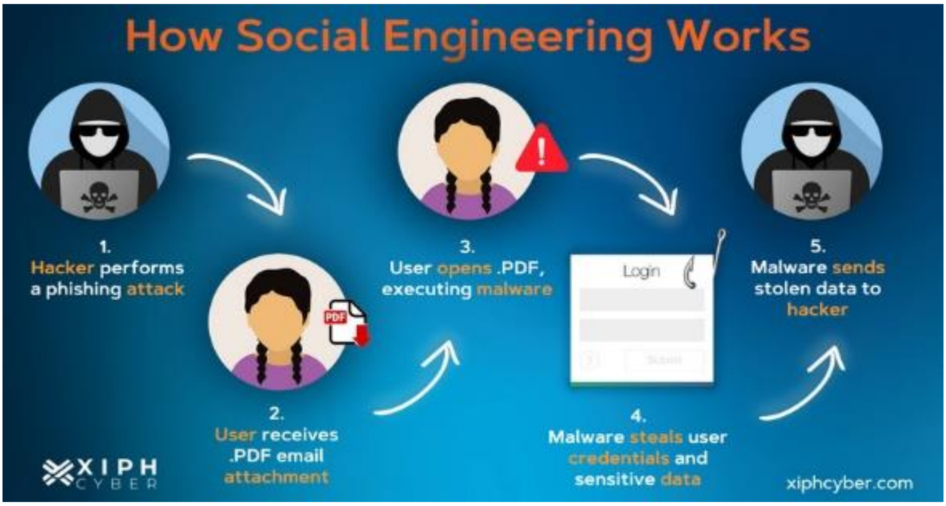


Source: spiceworks.com

Since (these) organizations are investing heavily in technical defences, there’s a need to add a layer to plug. The weakest human link. This review lays the ground for the idea that behavioural insights have to be incorporated into cybersecurity frameworks meant to protect against these social engineering and phishing techniques.

1. Background of the study

In today’s digital age, the push towards cybersecurity has become equally important for all organizations and individuals who are exposed to numerous types of cyber threats. Phishing and social engineering attacks are usually soft because that’s often where the human vulnerability resides, rather than actually a pure technical exploit. Cybercrime solutions like firewalls, encryption, and intrusion detection systems have gotten more sophisticated, but so have the cybercriminals—and they have found a way around these defenses based on human actions or the cognitive process.


How Social Engineering Works
1. Hacker performs a phishing attack
2. User receives .PDF email attachment
PDF
3. User opens .PDF, executing malware
Login
Submit
4. Malware steals user credentials and sensitive data
5. Malware sends stolen data to hacker
XIPH CYBER
xiphcyber.com

Source: xiphcyber.com

For instance, phishing involves trying to force people to tell them something confidential (sometimes passwords or financial info) via emails or messages that are not real or websites that fake the real website. Trust, curiosity, fear, or more commonly urgency are also used via social engineering techniques to get the victim to do the attackers bidding (most often clicking on malicious links and sharing private information). What these attacks show is that human factors are fundamental to the cybersecurity problem.

Understanding why individuals fall for such schemes has become an important behavioral insight. To begin with, human vulnerability to being targeted is mainly because of cognitive biases, lack of cybersecurity awareness, and insufficiently trained or untrained organizations. Research into psychological and behavioral factors reveals patterns of behaviors that attackers seek for their advantage, including a tendency to follow authority figures, to react to emergency messages, and to trust messages that look ‘familiar.’

For this study, we want to specifically review and synthesize existing research on the human element in cybersecurity in the context of behavioral (as opposed to technical) solutions to phishing and social engineering attacks. We then leverage these insights to understand what strategies effectively mitigate human vulnerability and enhance organizational and individual resilience to these threats. Human behavior has to be factored into cybersecurity to build the infrastructure of holistic defense mechanisms that include psychological and technological countermeasures.

2. Justification

- High growth of Cyber Threats

Phishing and social engineering attacks are becoming more high frequency and sophisticated and are real threats to users and organizations. However, understanding the human element is important; attackers prey on cognitive biases and behavioural patterns to trick what is arguably the weakest link, the user.

- Human Behaviour in Cybersecurity

Phishing and social engineering attacks are becoming more frequent and sophisticated, posing significant risks to individuals and organizations. Understanding the human element is crucial, as attackers exploit cognitive biases and behavioral patterns to deceive users.

However, with all the advancements in cybersecurity technology, human error remains the top breach-related driver. Analyzing behavioral insights can determine what vulnerabilities exist and how to train and make clientele aware of them.• No Comprehensive Behavioral Studies (of any type) have been performed.

Phishing and social engineering attacks are becoming more frequent and sophisticated, posing significant risks to individuals and organizations. Understanding the human element is crucial, as attackers exploit cognitive biases and behavioral patterns to deceive users.

Despite technological advancements in cybersecurity, human error remains a leading cause of security breaches. Analyzing behavioral insights can help identify vulnerabilities and develop more effective training and awareness programs.

However, the majority of the existing literature relies on technical defenses, so it leaves a gap in understanding the psychological and behavioral factors influencing the susceptibility to these attacks. This thesis addresses that gap by integrating research from behavioral sciences and cybersecurity.• Economic and Social aspects of cyber attacks and social engineering attacks are becoming more frequent and sophisticated, posing significant risks to individuals and organizations. Understanding the human element is crucial, as attackers exploit cognitive biases and behavioral patterns to deceive users.

Despite technological advancements in cybersecurity, human error remains a leading cause of security breaches. Analyzing behavioral insights can help identify vulnerabilities and develop more effective training and awareness programs. Existing literature often focuses on technical defenses, leaving a gap in understanding the psychological and behavioral factors that contribute to susceptibility to these attacks. This study aims to fill that gap by synthesizing research from behavioral sciences and cybersecurity. They cause substantial financial loss to the organizations and they damage their reputations. This study could therefore contribute to mitigating these impacts by learning from the human factors involved.And in need of Targeted Intervention Strategies.Phishing and social engineering attacks are becoming more frequent and sophisticated, posing significant risks to individuals and organizations. Understanding the human element is crucial, as attackers exploit cognitive biases and behavioral patterns to deceive users.Need for Targeted Intervention Strategies

Usually, traditional cybersecurity training is one size fits all. This study□s insights can enable the design of personalized interventions and educational campaigns for singular user profiles, behaviours, and experiences. Organizational Practices and Policy Development pollicising and social engineering attacks are becoming more frequent and sophisticated, posing significant risks to individuals and organizations. Understanding the human element is crucial, as attackers exploit cognitive biases and behavioural patterns to deceive users.

- Policy Development and Organizational Practices

Understanding the human aspect of cybersecurity is vital for policymakers and organizations to develop robust strategies. This research can inform guidelines, policies, and best practices to enhance security frameworks.

- Support for Multidisciplinary Approaches

Phishing and social engineering are addressed when cybersecurity professionals, behavioral scientists and educators collaborate. Consequently, this study demonstrates a need for an interdisciplinary approach towards dealing with complex human-centric threats. Academic and practical knowledge contributiong and social engineering attacks are becoming more frequent and sophisticated, posing significant risks to individuals and organizations. Understanding the human element is crucial, as attackers exploit cognitive biases and behavioral patterns to deceive users.

- Contribution to Academic and Practical Knowledge

This study could enrich the academic literature not only by concrete applications for universities but also by a comprehensive review of cyber security behavioral factors. In addition, it has industrial applications, providing actionable learnings for improving security awareness and minimising human errors in cybersecurity defenses.

3. Objectives of the Study

1. To analyze how human behavior and decision-making impact the effectiveness of cybersecurity measures, particularly in the context of phishing and social engineering attacks.
2. To investigate the psychological and social factors that make individuals and organizations vulnerable to phishing and social engineering tactics.
3. To evaluate the role of cybersecurity awareness and training programs in mitigating human vulnerabilities and improving defense mechanisms against such attacks.
4. To trace the development and sophistication of phishing and social engineering strategies over time and their implications for cybersecurity.
5. To propose practical, behavior-focused solutions and best practices for organizations and individuals to reduce the success rates of phishing and social engineering attacks.

4. Literature Review

Cybersecurity threats increasingly work through human vulnerabilities rather than technical weaknesses. However, studies reveal that human factors are a substantial part of successful cyberattacks, mainly using phishing and social engineering techniques. Attacks on systems are orchestrated by humans, who factor cognitive biases and decision-making processes into play (Hadnagy, 2018). To develop effective defense strategies, we need to understand these behavioral patterns.

Phishing continues to be one of the most common ways to take advantage of human vulnerability. It has been proven by research that phishing makes use of psychological manipulation, for example, urgency, authority, fear, etc, in order to manipulate an individual into giving away his personal sensitive information (Jampen et al., 2020). Email design, timing, and perceived legitimacy of the sender make phishing schemes successful

(Arachchilage & Love, 2014).

They also prove to be more vulnerable to these attacks for those with limited exposure to phishing simulations or relatively low cybersecurity awareness. Yet, exposure to phishing simulations repeatedly can enhance the ability of users to detect phishing, leading to a reduction of their vulnerabilities (Canham et al., 2022).

Social engineering abuses psychological rules and cognitive biases in order to get individuals to carry out activities that endanger security. Trust is also leveraged through techniques like: Pretexting, Baiting and Tailgating — all of which use social norms to gain unauthorized access (Mitnick & Simon, 2011). At certain factors, such as the authority bias, reciprocity, or the halo effect, they make it more likely to obey malicious requests.

Research has come out in recent times focusing on emotional manipulation as an important component in social engineering attacks. Workman (2008) states that attackers frequently exploit human emotions to skew reasoning and induce their targets to make a decision in the heat of a fearful or otherwise excited moment. And these tactics underline the need for training programs that train employees to recognise and resist manipulation.

With regards to human related cybersecurity risks, training and awareness initiatives have shown themselves to be successful. Phishing simulation, interactive workshop, and gamified training program interventions improve users' ability to identify and respond to phishing and social engineering attempts (Bada et al., 2019). Continuous training, and one trained for him rather than targeting a general population, seems to be more effective than single insightful interventions.

In addition, behavioral insights can be incorporated into training program that teaches the person about cognitive biases, emotional triggers, and these ideas will increase resilience against the social engineering tactics (Ngo & Nurse, 2020).

The attributional biases and other factors of human psychology and neurophysiology, which also shed light on insights from the psychology and neuroscience, are powerful methods of understanding and predicting how humans will respond to cyber threats. Predictive models can analyze user behaviour (response times, decision making) to identify individuals at higher risk of failure to the phishing or the social engineering (Jakobsson & Myers, 2007). The fact is, these models also allow organizations to create their cyber security strategy and make effective resource allocation.

While great strides have been made in understanding the human factor in cybersecurity, much remains to be understood. The one issue is human behavior is dynamic, it changes according to new threats and training interventions. Furthermore, keeping security in check along with keeping the user convenience and privacy is continuing challenge (Herley, 2009). While the training programs developed are effective for current military environments, future research should concentrate on creating adaptive programs that will grow and adapt to changing threat landscapes. The combining of behavioral science with more advanced technologies including machine learning and artificial intelligence can take this capability even further for cybersecurity systems.

Phishing and social engineering attacks are heavily powered by the human factor and that is a very important aspect in the cybersecurity landscape. Behavioral insights give us an insight into why people unwittingly engage with these attacks and how they can be taught to avoid them. These insights aid organizations to create more powerful and adaptive defense strategies.

5. Material and Methodology

Research Design:

Signalling a systemic review of literature to synthesize existing knowledge about human factors in cybersecurity with particular relevance to understanding the behavioral aspects of Phishing and Social Engineering attacks. This design is suitable for aggregation and condensation of findings in the earlier studies and therefore to have a better overall idea of the subject. Qualitative and quantitative data gathered from peer reviewed journal articles, conference proceedings and reports have been integrated to reveal trends, patterns and most key findings in the field.

Data Collection Methods:

All the data for this research was retrieved from the reputable academic databases available such as Scopus, Web of Science, IEEE Xplore, and Google Scholar. Search terms like “human factor in cybersecurity,” “phishing attacks,” “social engineering in cybersecurity,” and “behavioral insights” and “cybersecurity awareness” were used. Refine the search results were employed with Boolean operators, such as AND, OR and NOT. Only articles published between 2010 and 2024 were prioritized to include the most recent and relevant studies. Citation tracking and manual searches of references in key papers were used to identify additional sources. The only full text articles considered were in English.

Inclusion and Exclusion Criteria:

Inclusion Criteria:

1. Reviews of studies dealing with human factors on cybersecurity, with focus on phishing and social engineering attacks.
2. Journal articles, conference papers and technical reports, have been peer reviewed.
3. The subsequent research analyze behavioral insights, such as user awareness, training programs, and psychological factors.

Exclusion Criteria:

1. Studies done with a technical focus, including purely on algorithm development or network security protocols.
2. Blogs, opinion pieces, and editorials, all nonpeer reviewed sources.
3. In languages other than English.
4. The research that lacks empirical data or theoretical frameworks on human factors related to cybersecurity.

Ethical Consideration:
The study follows ethical standards when it comes to systematic reviews. Data used in this study carries no primary data, hence there are no human participants and the institutional ethical approval is not necessary. Intellectual property rights are respected in all sources which have all been cited appropriately and no data manipulation has taken place. Review was conducted with transparency and rigor in sake of the credibility and reliability of findings.

6. Results and Discussion

1. Cybersecurity Human Behavior and Decision Making
The results show that human behaviour plays a key role when cybersecurity measures are effective, especially for phishing and social engineering. Cognitive biases like trust, urgency and authority can steer decision making and lead to a low guard against malicious tactics. For example, when overconfident with their ability to identify threats, users underestimate the risk associated when clicking on unfamiliar links. Furthermore, heuristic based decision making under time pressure generally results in errors that tend to make us vulnerable to attacks.

2. Factors Related to Vulnerability on the Psychological and Social Plan
Phishing and social engineering are subject to susceptibility involving several psychological as well as social factors at both individual and organizational levels. Key findings include:
Social Proof and Authority Bias: These biases are exploited by attackers to impersonate authoritative figures, or use peer influence to manipulate victims.

Emotional Manipulation: When phishing emails come, they tend to ignite in the reader a fear, a curiosity, an excitement — basically anything they can use to get them to act immediately.

Trust Dynamics: We are intrinsically trusting to something familiar or, seemingly, credible, and this greatly increases our vulnerability.
Likewise organizational culture comes in to play as environments that are not very aware of cybersecurity or that have weak communication channels are more prone to attacks.

3. Effects on Business Outcome of Cybersecurity Awareness and Training Programs
Human vulnerabilities are mitigated by the measurable impact cybersecurity awareness and training programs have. The study highlights that:

- Scenario based training that is regular improves recognition of phishing attempts.
- Gamified training methods for the training of cyber security content improve user engagement and improve the rate of the retention of used cyber security practices.
- Organizations with strong cybersecurity culture experience less attempted phishing attacks (suggesting more attention to reinforcement of cybersecurity principles might help).

Yet, training remains ill suited for diverse user profiles, and it still fails to adapt to their changing attack strategies.

4. Phishing and Social Engineering Tactics – Evolution and Sophistication

Phishing and social engineering are becoming increasingly sophisticated and increasingly hard to detect.

The research identifies the following trends:

- Spear Phishing and Whaling: However, this has resulted in a sharp increase in highly personalized attacks focused on a specific individual or a high profile executive.
- Use of AI and Automation: An attacker applies machine learning to craft reality looking phishing messages, as well as identify potential targets.
- Multi-Channel Attacks: Attackers exploit social media, SMS (smishing), voice calls (vishing) … in addition to email in order to diversify their tactics.

These advances still point to the problem that cybersecurity defenses will always have to evolve to meet the ever changing threat.

5. Best Practices and Solutions based on Behaviours

Based on the findings, several practical solutions and best practices are proposed:

- Behavioral Interventions: Nudges, namely warning messages and confirmation prompts, can serve to interrupt automatic response and to persuade to make a conscious decision when to implement.
- Phishing Simulation Exercises: Regular simulations reinforce vigilance and provide feedback actionable by users.
- Multi-Factor Authentication (MFA): By encouraging the use of MFA, you’re attacking the big problem of compromised credentials, adding an extra layer of security.
- Continuous Education and Feedback Loops: Cybersecurity training should not be a one and done event, it should be a continuing process that learns from past incidents and developing threats.

And encouraging organizations to cultivate a cyber security mindfulness culture empowers and holds employees responsible for protection of digital assets.

7. Limitations of the study

1. Scope of Literature Reviewed: The major part of the study is derived from the existing literature to know the insights on the human behavior in the context of cybersecurity and what is the focus is on phishing and social engineering. These are dependent on the quality and the comprehensiveness of the existing studies which vary methodology and context.
2. Focus on Behavioral Aspects: Although this paper does focus on behavioral insights, it does not deeply engage with countermeasures that are technically motivated or next generation cybersecurity technology. However, this narrowed focus may very well create the possibility to ignore the interrelationship between human and technical factors that has been suspected for thwarting phishing and social engineering threats.
3. Geographic and Cultural Limitations: Most of the reviewed studies are based on data from particular geographic regions or a cultural context and as such can only be

generalised across other regions where there are different levels of cybersecurity awareness, different levels of attitudes towards technology, or different cultures.

4. Dynamic Nature of Cyber Threats: The timeliness of the findings challenge tradecraft in this rapidly changing cyber threat landscape. The dinosaurs of the past are already in the process of fading from the scene, and some of the findings may not be applicable as new and newer creations of new social engineering techniques and phishing method appear.
5. Lack of Empirical Validation: Due to insufficient existing empirical investigations, this study is a review paper, synthesizing existing research on CCP. This absence of direct experimentation or data collection could lead to less robust conclusions drawn.
6. Diversity of Target Populations: Most of the studies reviewed focus on specific demographics such as corporate employees or university students and fail to access the population at large. However, such limitation may restrict applicability of the insights to other user groups.
7. Psychological and Contextual Variations: Human behavior in the area of cybersecurity falls into a wide spectrum of psychological and situational factors, stress, urgency, environmental conditions. The variety of such variations, however, may prevent one from accounting for all, placing a limit on the depth that one can carry out an analysis.
8. Potential Publication Bias: As a function of publication, the published research upon which the study relies may be biased. Whole nulls are often pushed to the side in favor of nice positive findings or new insights at the expense of synthesis.

8. Future Scope

Given the concerning sophistication of phishing and social engineering attacks continuing to fund research in this domain to uncover human factors that lead to cybersecurity vulnerabilities is justified. Future studies can explore the following areas to enhance understanding and mitigation strategies:

1. Advanced Behavioral Models: Specific models that will predict susceptibility to phishing and social engagement can be developed in attempting to integrate psychological and behavior sciences. It will involve studying cognitive biases, stress factors and decision making methods, that are abused by attack vectors.
2. AI-Driven Personalization: You can employ artificial intelligence and machine learning to use the designing of individualized security training plans to match people's learn rate and risk level to make people of the potential threats and how they should respond to them.
3. Impact of Emerging Technologies: Future work could study how, and how best to use virtual reality, augmented reality, and the metaverse, as all of these technologies will only grow in use and see more widespread adoption.
4. Cross-Cultural Analysis: Phishing and social engineering attacks do not operate within boundaries, so analysis of variations in the victim dispositions within different cultural and regional demographics can aid in designing phishing and social engineering defenses accordingly.

5. Policy and Ethical Considerations: The world of human behavior is stepped into the shadow world of human behavior in the name of cybersecurity: research on the ethical implications, and guidelines for mitigating privacy concerns during proactive threat management.
6. Neuroscience Applications: If one combined neuroscience and cybersecurity, there are insights to gain from the neural mechanisms of decision making and impulsivity, and how people get lost to attacks.
7. Gamification and Immersive Training: This thesis suggests that future studies can test the gamified and immersive simulations for higher levels of user engagement and retention of cybersecurity best practices as dictated by the findings of this thesis.
8. Longitudinal Studies: With this work, long term studies can now be conducted to explore the long term effectiveness of behavioral interventions over time that can help refine strategies and identify long terms solutions to reduce phishing and social engineering thefts.

9. Conclusion

This study suggests that Human Factors are very important to cybersecurity, especially to the extent that phishing and social engineering attacks depend on those factors. We determine that technological defenses are necessary, but not sufficient, and that defenders must fix the behavioral weaknesses attackers exploit.

The vulnerability of people to phishing and social engineering resides primarily in inbuilt cognitive biases in decision making under pressure. However, all these biases, including trust, authority, and urgency make human behavior a human hard to defeat weak link to cybersecurity effectiveness.

Psychological manipulation is at the heart of phishing and social engineering as it remains. Authority bias, peer influence, emotional triggers like fear, curiosity and excitement, all beat social factors and are amplified even further, making a successful attack a far higher probability. In addition, vulnerabilities from organization factors result from poor communication and poor cybersecurity culture.

In addition to this, awareness and training for the programs reduced the human vulnerabilities. Several studies show that with frequent, interactive training as it relates to context, users can learn to tell phishing from legit and to reply correctly. For example, these programs employ gamification and real world simulations to further amplify the effect in which employees become imbued with proactive security mindset.

In addition, phishing and social engineering methods have become sophisticated over time, attackers began to use advanced method like personalized (AI), multi channel attacks and spear phishing. It becomes increasingly obvious that we need dynamic and adaptive defense strategies to learn how to prepare for and defend against new attack vectors.

A behavior focus solution is the only way to fight phishing and social engineering attacks. Interventions have led such as, warning systems, regular phishing simulations and use of multi factor authentication, are some. It’s an ongoing education for the users, with feedback loops, to guarantee the users get to know about best practices and emerging threats.

The work backs the need for a two pronged approach to address technological defenses and behavioral insights. A priority is to build a cybersecurity aware culture through educating and enabling your staff to collaborate to protect your organisation. In point of fact, sustaining that extra step ahead of all advanced attack strategies will require ongoing investment in advanced training programs and the development of adaptive defense systems.

Cybersecurity’s human factor is an auxiliary measure to be foreseen but actually core to good defense strategies. Phishing and social engineering attacks are growing, so organizations and people need to be on guard. By integrating behavioral insights and the innovation of technology we can significantly bolster the cybersecurity ecosystem by reducing attack success rates and enhancing overall organizational resiliency.

References

1. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. Communications of the ACM, 42(12), 40-46.
2. Albladi, S. M., & Weir, G. R. S. (2018). Predicting individuals’ vulnerability to social engineering in social networks. Cybersecurity, 1(6), 1-12.
3. Arachchilage, N. A. G., & Love, S. (2014). A game design framework for avoiding phishing attacks. *Computers in Human Behavior, 29*(3), 706-714.
4. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behavior? *arXiv preprint arXiv:1901.02672*.
5. Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the effectiveness of cybersecurity awareness campaigns. Journal of Cybersecurity, 4(1), 1-12.
6. Bullee, J.-W. H., Montoya, L., Junger, M., & Hartel, P. H. (2018). Spear phishing in organizations: Influence of organizational maturity and knowledge on susceptibility. Journal of Cybersecurity, 4(1), 1-15.
7. Canham, M., Vance, A., & Siponen, M. (2022). The effectiveness of repeated phishing training: A longitudinal field study. *Journal of Management Information Systems, 39*(1), 1-31.
8. Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 581-590.
9. Ferreira, A., Correia, R., & Simões-Marques, M. (2015). The influence of information security culture on information security decision-making. International Journal of Information Management, 34(3), 344-355.
10. Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), 983-988.
11. Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. Journal of Cyber Security and Information Systems, 8(3), 29-36.
12. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.
13. Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. Computers in Human Behavior, 30, 294-304.
14. Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the 2009 Workshop on New Security Paradigms*, 133-144.
15. Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. Proceedings of the New Security Paradigms Workshop, 133-144.

16. Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74-81.
17. Jakobsson, M., & Myers, S. (2006). Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. Wiley.
18. Jakobsson, M., & Myers, S. (2007). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley.
19. Jampen, D., von Solms, R., & Kritzinger, E. (2020). An analysis of phishing attacks and their detection. *Journal of Cybersecurity, 6*(1), 1-12.
20. Jansson, K., & Von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584-593.
21. Jones, H., & Colwill, C. (2007). Human factors: Understanding people in the cyber domain. Information Security Technical Report, 12(3), 109-114.
22. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology, 10(2), 7-21.
23. Langton, K., Kankanhalli, A., & Tan, B. C. Y. (2016). Understanding susceptibility to social engineering in the workplace. Journal of Management Information Systems, 33(2), 362-389.
24. Marett, K., & Joshi, K. D. (2009). The decision to share information and rumors about threats: An extension of protection motivation theory. MIS Quarterly, 33(1), 123-142.
25. Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. Wiley.
26. Mitnick, K. D., & Simon, W. L. (2011). *The Art of Deception: Controlling the Human Element of Security*. Wiley.
27. Ngo, H. H., & Nurse, J. R. (2020). A behavioral analysis of susceptibility to phishing attacks. *Human Factors, 62*(5), 1-15.
28. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176.
29. Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), 597-611.
30. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.
31. Sun, J. C.-Y., & Wang, Y.-C. (2012). Social engineering tactics and human psychological manipulation. CyberPsychology, Behavior, and Social Networking, 15(12), 711-718.
32. Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of phishing: Examining the roles of persuasion, personality and embarrassment. Journal of Human Behavior in IT, 3*(2), 203-223.
33. Vishwanath, A., Harrison, B., & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. Journal of Management Information Systems, 33(4), 865-891.
34. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. Cyberpsychology, Behavior, and Social Networking, 22(3), 194-199.
35. Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.