JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

HUMAN BEHAVIOUR AND CYBER SECURITY: BRIDGING THE GAP BETWEEN TECHNOLOGY AND PSYCHOLOGY

Deepika Poojari[1], Asst. Prof. Gauri Mhatre[2]
[1]Student, [2]Guide
[1]Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India
[2]Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

Abstract*— This study paper aims to shed light on the critical role that human factors play in the digital security landscape. Understanding the delicate connection between human behaviour and cyber security has become critical in an era marked by growing cyber threats. We uncover the complexity that underpin user activities in cyberspace by diving into the domains of psychology, cognitive biases, and decision-making processes. The ethical concerns of data collection and privacy issues are also examined. This article also investigates the efficacy of security awareness campaigns, the trade-offs between usability and security, and the emerging topic of user-centric security technology. We demonstrate the concrete impact of human behaviour on cyber security results using a variety of case studies and actual evidence. Finally, this study provides valuable insights and recommendations for strengthening organizations' and individuals' resilience to evolving cyber threats, emphasizing the critical need for a holistic approach that bridges the gap between technology and psychology in safeguarding the digital realm.

***Keywords*—Human Psychology, Cyber Security, Technology, Phishing, Authentication, Awareness, etc.**

1. INTRODUCTION

As we see the constant growth of cyber threats, it becomes clear that technology alone cannot provide a strong defence against the creative ability of bad actors. In an era defined by constant connection and digital transformation, technology affects almost every part of our lives. Individuals must constantly negotiate a digital landscape loaded with potential perils, from falling victim to sophisticated phishing attempts to unwittingly releasing important information. This technical immersion, while providing amazing ease and productivity, also creates a slew of cyber security challenges. As a result, this study aims to establish a connection between psychology and technology by unravelling the intricate interplay of human elements in the context of cyber security. Cyber Security is not just a technical issue it is also a human issue.

According to Verizon's 2021 Data Breach Investigations Report, 85% of successful cyber-attacks now involve a human element. Combine that with the fact that even the very best technology can only thwart about 93% of attacks, and that leaves a large hole in an organization's basic security hygiene [1]. So the Cyber security training has become very essential instead of being just as optional training. Just giving the people the same training won't solve the problem since each one has a different understanding and it might fall short.

2. THE HUMAN ELEMENT IN CYBER SECURITY:

There are different reasons due to which the cyber security is compromised i.e. Phishing and Social engineering, Cyber Security Awareness and education, Password Practices and Authentication, Insider Threats, Human Error, BYOD Policies, Cultural and Organizational factors, etc. Phishing emails may claim that their account or personal information is at risk, focusing on the user's fear of losing access or privacy.

Phishing attacks regularly employ psychological approaches to trick people into disclosing sensitive information such as passwords or financial information. Phishers can induce fear by claiming that quick action is essential to avoid bad repercussions (for example, account dismissal, a lawsuit, or security issues). Emails sent by phishing sites may contain urls that appear to be authentic at first sight but really route consumers to malicious websites meant to steal critical information.

To establish confidence and credibility, phishers may act as a legitimate company, institution, or individual in power, such as a bank, a government organization, or IT support. Ongoing training emphasizes the significance of creating unique, reliable passwords and the need to revise them on a frequent basis. Individuals can be trained about common phishing techniques through regular training sessions, allowing them to spot and avoid questionable emails or texts. Continuous training promotes a security culture in which leadership highlights the necessity of cyber security, instilling a sense of shared responsibility in all employees. Social engineering cyber-attacks trick the user into infecting their own device with malware [2].

3. CYBER SECURITY PSYCHOLOGICAL FRAMEWORKS:

It focuses on educating the users about the cyber security threats and promoting security culture along with the training to enhance user's ability to recognize and respond to potential risks. Unique patterns of behaviour, that include keystrokes and mouse movements, are used for authenticating users and adding an extra layer of security. It highlights the part that human behaviour plays in cyber security events. Acknowledging that people serve as both targets and participants to security risks. In order to address privacy concerns on personal data, and encourage ethics in using artificial intelligence and other cyber security techniques. Use game-like training to make learning more engaging and motivating, which will encourage people to participate actively. As individuals and organizations experience the many facets of cyber security in their everyday lives, it's clear that psychological motivations and effects vary [3].

4. METHODOLOGY

In order to gather data on people's mindfulness, we first polled those who used online form generators and data collection services. People's beliefs can be determined using the thorough disquisition. It assists in discovery of anomalies and implicit pitfalls from inside by looking at user behaviour and psychographic characteristics.

5. ANALYSIS AND DISCUSSION DATA COLLECTION

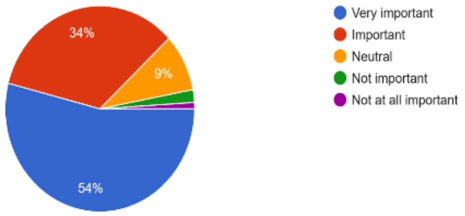
The survey is used to gather the data. Both the outcome and the process by which it was arrived at will be examined. In this instance, 100 people were asked their opinions on the subject of "Human Behaviour and Cyber Security: Bridging the Gap between Technology and Psychology." The survey is necessary to obtain high-quality data that can subsequently be examined and used to determine the survey's outcome. By employing the survey research method, the study would obtain high-quality data by asking the appropriate questions of the appropriate people, who were between the ages of 18 and 30, in order to proceed with the survey.

QUESTIONNAIRE

- How do you perceive the role of psychology in enhancing cyber security measures?
- Do you use unique passwords for different online accounts?
- Have you ever used two-factor authentication for your accounts?
- Do you feel stressed or anxious about your online security?
- How likely are you to share personal information online?
- Which of the following psychological factors do you think is most critical for improving cyber security?
- Do you believe that incorporating psychological principles into cyber security measures can enhance overall security?
- Do you think human behaviour plays a significant role in cyber security incidents?
- On a scale of 1 to 5, how confident are you in your ability to recognize phishing emails or messages?
- Have you ever fallen victim to a cyber-attack or online scam?
- Which of the following do you believe is the most common cyber security threat?

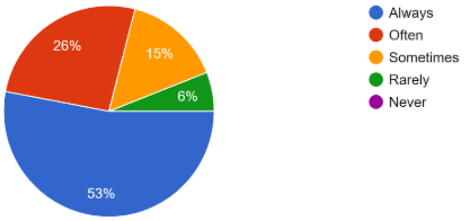
RESULTS

1.



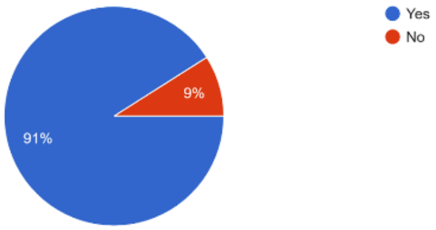
When the people were asked regarding the role of psychology, 54% said it is very Important, 34% said it is Important, 9% said it is Neutral, 2% said Not Important & 1% said it is Not at all important.

2.



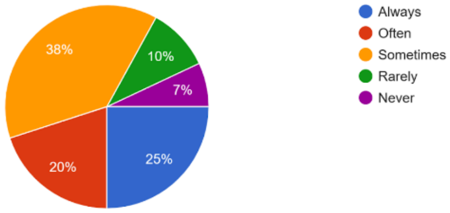
When they were asked if they use unique passwords for different accounts, 53% said always, 26% said often, 15% said Sometimes, 6% said rarely & 0% said never.

3.



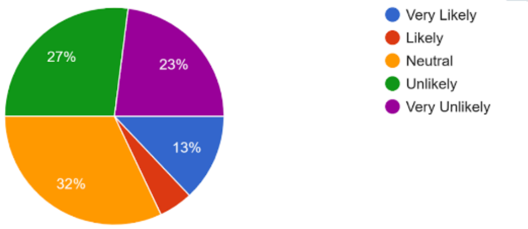
When they were asked if they use two factor authentication for their accounts, 91% said yes & 9% said no.

4.



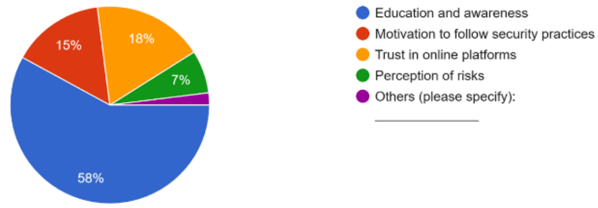
When they were asked if they feel stressed or anxious about their online security, 25% said always, 20% said often, 38% said sometimes, 10% said rarely & 7% said Never.

5.



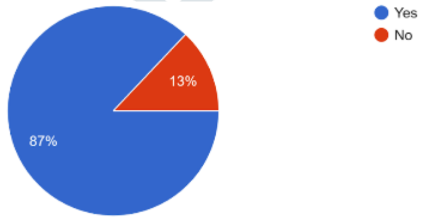
When they were asked if they are likely to share personal information online, 13% said Very likely, 5% said likely, 32% said Neutral, 27% said Unlikely & 23% said Very Unlikely.

6.



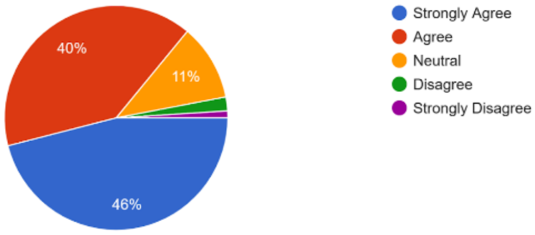
When they were asked according to them what is the most crucial physiological factor for improving cyber security, 58% said Education and awareness, 15% said Motivation to follow security practices, 18% said Trust in online platforms, 7% said Perception of risks & 2% said others.

7.



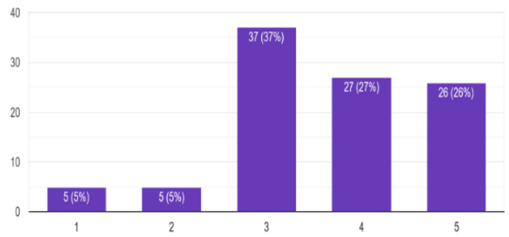
When they were asked whether incorporating psychological principles into cyber security measures enhance overall security, 87% said yes & 13% said no.

8.



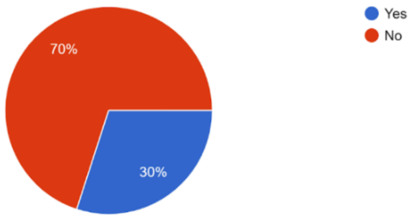
When they were asked if human behaviour plays a significant role in cyber security incidents, 46% strongly Agreed, 30% Agreed, 11% said Neutral, 2% Disagreed & 1% said Strongly Disagreed.

9.



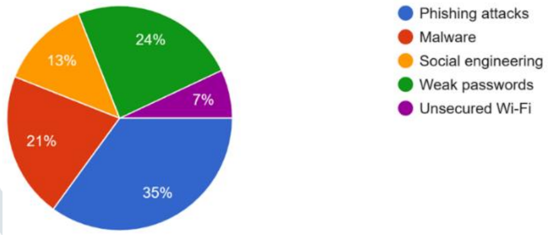
When they were asked about the confidence level of recognizing phishing emails or messages in scale for 1(not confident at all) to 5(very confident), 5% answered 1, 5% answered 2, 37% answered 3, 27% answered 4 & 26% answered 5.

10.



When they were asked if they have ever fallen victim to any online scam, 70% said yes & 30% said no.

11.



When they were asked about the most common cyber security threat, 35% said Phishing attacks.21% said Malware, 13% said Social Engineering, 24% said Weak Passwords & 7% said Unsecured Wi-Fi.

HYPOTHESIS TESTING

Hypothesis testing is a way of statistical reasoning that includes analysing the data from the samples to drive statistical inferences to conclude population parameters or probability distribution. First, the hypothesis or assumption is a claim regarding the population parameter or probability distribution, which is known as the null hypothesis. Its id was donated by H0. After that alternate hypothesis is defined. It is donated by Ha. The alternate hypothesis is defined, as the opposite of the null hypothesis. By using sample data, the hypothesis testing technique which determines whether or not H0 may be rejected. If H0 is rejected, the statistical conclusion is that the alternate hypothesis Ha is true.

For this paper,
Null hypothesis (H0): μ = Human behaviour has an important effect on cyber security results, so improving cyber security measures will require bridging the technology and psychology divide.

The alternate hypothesis (Ha): μ ≠ Human behaviour and cyber security results are not strongly related, and attempts to close the divide between technology and mental health will not lead to better cyber security practices.

TEST (Statistics)

There are three types of tests available to determine the given
Assumption the null hypothesis is rejected or accepted.

The type of test is as follows:

- Chi-squared test
- T-student test
- Fisher’s Z-test.

For this paper, we are using 2two tailed T-student tests.

A t-test is an inferential statistic that determines if there is a significant difference in the means of two groups that are related in some manner.
Level of significance

The chance of rejecting the null hypothesis when it is true is the significance level (also known as alpha or α). A significance level is 0.05 for the example, which means there is a 5% of probability of discovering a difference when there is not one. Lower significance levels indicate that more evidence is required to reject the null hypothesis.

Level of confidence

The confidence level indicates the probability that the location of the statistical parameter (such as the arithmetic mean) measured in the sample survey is also true for the entire population.

Index	Data(m)	(m-x)	$(m-x)^2$
1	54	-2.36364	5.586777
2	53	-1.36364	1.859504
3	91	-39.3636	1549.496
4	25	26.63636	709.4959
5	23	28.63636	820.0413
6	58	-6.36364	40.49587
7	87	-35.3636	1250.587
8	46	5.636364	31.7686
9	26	25.63636	657.2231
10	70	-18.3636	337.2231
11	35	16.63636	276.7686
$\sum X$	568		$\sum(m-X)^2$
			5680.55

$\sum X = m/n = 568/11 = 51.64$

S.D (S) = $\sqrt{\sum}$ (m - X)2/n – 1 = 23.83

A t-score (t-value) is the number of standard deviations away from the t-mean.

The formula to find a t-score is:

$T = (X-\mu) /(S/\sqrt{n})$

Where X: is the sample mean,

μ: is the hypothesized mean, S: sample standard deviation, n: sample total population.

The p-value, also known as the probability value, indicates how probable your data is to have happened under the null hypothesis. Once we know of t, we can find the corresponding p-value. If the p-value is less than some alpha level (common choices are 0.01, 0.05, 0.10) then we can reject the null hypothesis

Calculation of T-value:

Step 1: Determine the null hypothesis and alternate hypothesis are.

Null hypothesis (H0): Human behaviour has an important effect on cyber security results, so improving cyber security measures will require bridging the technology and psychology divide.

The alternate hypothesis (Ha): Human behaviour and cyber security results are not strongly related, and attempts to close the divide between technology and mental health will not lead to better cyber security practices.

Step 2: find the test statistic.

In this case, the hypothesis mean value is

$|t|= (X-\mu) /(S/\sqrt{n})$

$= (51.64 – 75)/ (23.83/\sqrt{11})$

$|t|= 3.25$

t-value = 0.11

Calculating pvalue:

Step 3: calculate the test statistic’s p-value.

The t-Distribution table with n-1 degree of freedom is used to calculate the p-value. In this paper, the sample size is n=11, so n-1 = 10.

Level of significance (α) =0.05

Tabulated t at 10 degrees of freedom and α = 0.05

Level of significance for two-tailed test t=2.201

Since the t-value is less than our chosen alpha level of 0.05, we can accept the null hypothesis. Thus, Human behaviour has an important effect on cyber security results, so improving cyber security measures will require bridging the technology and psychology divide.

6. FUTURE DIRECTIONS AND CHALLENGES:

In a constantly changing situation of technology, psychology and cyber security, several trends are expected to emerge. For the identification of users, a greater emphasis will be put on behavioural biometrics that can take advantage of unique user behaviour patterns. Secondly, the role of Human Error in security incidents is going to be addressed through increased emphasis on cyber safety centric training by humans. Thirdly, the overall user experience and compliance are improved by using psychology principles when designing user friendly security interfaces. Fourth, earlier identification of potential risks will be helped by advances in the use of psychological profiling to identify threats. Fifth, adaptive threat detection and response based on psychological models will be facilitated by a greater use of intelligence in cyber security solutions. Sixthly, top priority will be to address privacy concerns related to psychographic data and the application of ethics in artificial intelligence. Finally, the development of online psychology as a specialized field will examine the emotional impact of technology on individuals, which will contribute to a greater awareness of cyber security challenges.

7. CONCLUSION

To summarize, it is a fundamental link that requires the attention and collaboration between technology and psychology in order to address this intersection of humans' behaviour with cyber security. Understanding people's interaction with digital environments, making decisions and responding to security measures will be essential in a changing landscape of cyberspace. In order to develop and implement effective cyber security strategies, the gap between technology and psychology needs to be bridged. In designing systems that not only protect against external threats, but also take into account the complexity of human cognition, emotion, and behaviour, it is essential to recognise the human element as both a vulnerability and a strength. Successful cyber security solutions cannot rely only on technical progress, as shown by this synthesis.

REFERENCES:-

[1] S. Moramarco, “Behavioral psychology training reduces cybersecurity risks,” 16 February 2022. [Online]. Available: https://www.securitymagazine.com/articles/97093-behavioral-psychology-training-reduces-cybersecurity-risks.

[2] “University of Central Florida,” [Online]. Available: https://digitalskills.ce.ucf.edu/cybersecurity/social-engineering-attacks-the-what-why-and-how/.

[3] “The Psychology of Cybersecurity,” 30 October 2019. [Online]. Available: https://www.crowe.com/cybersecurity-watch/psychology-of-cybersecurity.