

Original Research

Received 01 July 2026

Revised 09 Aug 2026

Accepted 22 Aug 2026

Natural Resources for Human Health 2026, Vol. 6 (17s): 802–813

KEYWORDS:

Cyber security awareness, digital privacy, protection motivation theory, technology acceptance model, engineering students, information security behaviour, self-efficacy.

Cybersecurity Awareness and Digital Privacy Behaviour Among Engineering Students: An Empirical Study Using an Extended Protection Motivation Theory–Technology Acceptance Model Framework

V. Harshavardhan¹, C. Rani², J. S. Ananda Kumar³, Kandati Sai Chandu⁴, Khaja khan pathan⁵, P. Balaji⁶

¹Associate Professor, Department of MCA, Siddharth Institute of Engineering & Technology, Puttur, 9959974091, vemuriharsha@gmail.com

²Associate Professor, Department of MBA, Siddharth Institute of Engineering & Technology, Puttur, 9959974091, poori.rani@gmail.com

³Associate Professor, Department of MCA, Siddharth Institute of Engineering & Technology, Puttur, 9959974091, jsanandkumar@gmail.com

⁴Associate Professor, Department of MBA, Siddharth Institute of Engineering & Technology, Puttur, 9550886140 drkandatisaichandu@gmail.com

⁵SAP consultant, Infosys limited, India. 965250556

⁶Associate Professor, Department of MCA, Siddharth Institute of Engineering & Technology, Puttur, 9885482633, sietkmca.balaji@gmail.com

ABSTRACT: Engineering undergraduates now rely heavily on internet-enabled devices, cloud-based academic platforms and social media, which makes cyber security awareness and digital privacy behaviour essential skills for the twenty-first century. This study investigates the level of cyber security awareness, perceived threat, self-efficacy and security behaviour among Bachelor of Technology (B. Tech) students in India, and examines the psychological predictors of their protective behaviour and behavioural intention. An integrated model was used in which Protection Motivation Theory (PMT) constructs are combined with constructs borrowed from the Technology Acceptance Model (TAM). Data from 186 engineering undergraduates in their second, third and fourth years were gathered through a structured questionnaire covering ten constructs: Knowledge/Awareness, Perceived Severity, Susceptibility, Benefits, Self-Efficacy, Usefulness, Ease of Use, Privacy Concern, Protective Behaviour and Behavioural Intention. Every construct showed good to excellent reliability (Cronbach's $\alpha = 0.82$ – 0.93 ; overall $\alpha = 0.98$). Mean scores were moderately positive (3.61–3.89 on a 5-point scale), lowest for Perceived Ease of Use and highest for Perceived Benefits. One-way ANOVA revealed that scores for Knowledge, Perceived Susceptibility, Ease of Use, and Privacy Concern increased significantly over study years ($p < .05$), while independent-samples t-tests revealed that female respondents scored significantly higher than male respondents on Perceived Benefits, Usefulness, Ease of Use, and Behavioural Intention ($p < .05$). Previous participation in a cyber security workshop or course was the most influential demographic factor: attendees scored significantly higher on all ten constructs (all $p \leq .011$). Protective behaviour was significantly predicted by Self-Efficacy, Perceived Ease of Use, Perceived Usefulness, and Privacy Concern in multiple linear regression ($R^2 = .78$), while behavioural intention was significantly predicted by

Perceived Usefulness, Perceived Susceptibility, Perceived Severity, and Perceived Ease of Use ($R^2 = .63$). The results provide India-specific evidence to guide the design of cyber security education in institutions and future PMT-based research on behaviour change in higher education.

1. INTRODUCTION

Smartphones, cloud-based learning management systems, digital payments and social media have transformed how engineering students study, interact and handle their personal data. According to the National Crime Records Bureau (NCRB) under the Ministry of Home Affairs (MHA), registered cybercrime cases in India grew by 17.9%, from 86,420 in 2023 to 101,928 in 2024. The national rate climbed from 6.2 to 7.3 cases per lakh population over the same period, and cyber fraud made up 72.6% of all cases registered in 2024 (NCRB, 2025). University students are heavily connected, spending much of their time online for study, social life and financial transactions, yet they are poorly prepared to recognise and resist common attack vectors such as phishing, credential theft and social engineering (Alqahtani, 2022a; Senthilkumar and Easwaramoorthy, 2017).

Engineering students deserve particular attention because the security habits they form now are likely to shape the security culture of the workplaces they later join (Pósa & Grossklags, 2022). Yet understanding a threat does not automatically produce protective action. A substantial body of work describes an “awareness–behaviour gap”: people who know about phishing, malware and multi-factor authentication (MFA) still reuse passwords, postpone software patches and open suspicious links (Bognár & Bottyán, 2024; Rohan et al., 2023). Explaining why knowledge fails to translate into secure behaviour requires examining how students appraise threats, how confident they are in carrying out protective actions, and how useful and usable they find security tools.

To address this need, the study brings together two widely used behavioural theories from information-security research. Through threat appraisal (perceived severity and susceptibility) and coping appraisal (perceived benefits of the protective action, response efficacy, and self-efficacy), Protection Motivation Theory (PMT) explains protective action (Rogers, 1975). The Technology Acceptance Model (TAM) explains the acceptance of security systems on the basis of their perceived usefulness and perceived simplicity of use (Davis, 1989). Using a single validated instrument, the study tests which psychological factors are most closely tied to actual protective behaviour and future intention among Indian engineering undergraduates, a group under-represented in international research compared with students in the United States, China and Europe, and it combines these constructs with knowledge/awareness, privacy concern, protective behaviour and behavioural intention.

2. LITERATURE REVIEW

2.1 Cybersecurity awareness among university students

Student cybersecurity awareness has been examined in many national contexts. Chandarman and Van Niekerk (2017) surveyed students at a private tertiary institution in South Africa and reported generally positive self-reported awareness, although password practices and the perception of risks on public Wi-Fi were weak points. Senthilkumar and Easwaramoorthy (2017) similarly observed that engineering students in Tamil Nadu, India, recognised familiar threats such as viruses and phishing but were less familiar with technical ones, including man-in-the-middle attacks and risky app permissions. Alqahtani (2022a, 2022b) reported that knowledge of software security and e-mail security were significant positive predictors of overall cybersecurity awareness among Saudi Arabian university students, with software security explaining roughly 19% of the variance. More recently, Bognár and Bottyán (2024) developed and validated a Personal Cybersecurity Awareness Scale for university students using exploratory and confirmatory factor analysis; it yielded five behavioural dimensions and showed that Knowledge/Awareness and Protective Behaviour are related yet load on separate factors. This supports the decision in the present study to treat the two as distinct constructs.

2.2 Theoretical Frameworks

Rogers (1975) first proposed Protection Motivation Theory in the setting of health-related fear appeals, and it has since become a leading framework for explaining voluntary cyber security behaviour. The theory holds that protective behaviour

arises from a threat appraisal, comprising the perceived severity of the threat and perceived susceptibility to it, and a coping appraisal, comprising the perceived effectiveness or benefits of the protective response and self-efficacy, that is, belief in one's own ability to carry it out. In a controlled cyber security-training intervention with 154 undergraduates, Khan et al. (2023) identified self-efficacy as the main predictor of behavioural intention both before and after training. Han et al. (2025) reached a comparable conclusion in a large survey of 3,030 Chinese college students, in which threat-appraisal and coping-appraisal variables both significantly predicted information-security behaviour. The Technology Acceptance Model (Davis, 1989) was originally created to explain the adoption of software in the workplace. It is increasingly applied to cyber security because even an informed and motivated user is unlikely to adopt a protective tool, such as a password manager or multi-factor authentication, that seems hard to use or of little practical value. By combining PMT and TAM constructs in one instrument, the present study can directly compare threat-driven and usability-driven predictors of student security behaviour, a comparison seldom made in research on students.

2.3 Gender and Demographic Differences in Cybersecurity and Privacy Behaviour

The evidence on gender differences in cyber security awareness and privacy concern is inconsistent. García-Crespo et al. (2019) documented differences between male and female users in Internet-security habits and awareness. In a survey of 762 higher-education students from five countries, Kizilcec et al. (2023) found that women reported stronger trusting beliefs and a greater tendency toward self-disclosure than men, with the size of the effect depending on national context and degree programme. Bognár and Bottyán (2024), by contrast, found that men scored significantly higher on “Proactive Protection Behaviours” and “Secure Online Habits”, with no significant gender difference in personal-information protection or financial-cyber security awareness, which shows that gender effects depend on the specific construct rather than being uniform. Age and academic seniority have also been studied. Mai and Tick (2021) compared Hungarian and Vietnamese university students and found insufficient material knowledge of information security in both groups regardless of seniority, while Pósa and Grossklags (2022) reported that more self-reported work experience was linked to higher cyber-risk awareness among university students, implying that exposure, whether through employment or progress through a degree, matters.

2.4 The Awareness–Behaviour Gap and the Role of Formal Training

Across the cyber security-education literature, awareness-raising on its own is repeatedly found to be an incomplete intervention. In a systematic review of scales that measure information-security awareness, Rohan et al. (2023) observed that most instruments capture only the knowledge dimension and seldom measure the psychological antecedents of behaviour that PMT and TAM constructs are intended to assess. Parsons et al. (2014) applied the widely used Human Aspects of Information Security Questionnaire (HAIS-Q) to Australian employees and found that policy knowledge predicted attitude more strongly than actual computer-use behaviour, which supports treating behaviour and intention as outcomes separate from knowledge. Formal training has been more consistently effective. Khan et al. (2023) reported that a Kirkpatrick-model evaluation of PMT-based cyber security training produced significant gains in both threat knowledge and behavioural intention, and Antunes et al. (2021) showed that an integrated cyber-awareness strategy, combining attitude assessment, self-diagnosis and structured educational content, improved measurable security behaviour in a school setting. Together these results justify including in the present study a direct comparison of students who have and have not previously attended a cyber security course or workshop.

2.5 Research Gap and Contribution of the Present Study

Although research on cyber security awareness among university students is well developed internationally, India-specific evidence at the construct level remains limited for engineering undergraduates. This is especially true of work that, within one validated instrument, separately measures threat appraisal, coping appraisal, technology-acceptance constructs, privacy concern, and both actual protective behaviour and future intention. Most Indian studies so far (e.g., Senthilkumar & Easwaramoorthy, 2017) report descriptive awareness levels without testing a multi-construct behavioural model. This study addresses the gap in three ways: (i) it applies a ten-construct instrument grounded jointly in PMT and TAM to a sample of B.Tech engineering students; (ii) it uses multiple regression to test which constructs most strongly predict protective behaviour and behavioural intention; and (iii) it compares demographic and experiential factors (gender, year of study, prior workshop attendance and prior cyber attack experience) with the findings of existing international research. protective behaviour and behavioural intention through multiple regression, and (iii) benchmarking demographic and experiential

moderators (gender, year of study, prior workshop attendance, and prior cyber attack experience) against the existing international literature.

3. MATERIALS AND METHODS

3.1 Research Design

This study followed a cross-sectional, quantitative survey design. Data were gathered with one structured, self-administered online questionnaire, which allowed responses to be collected quickly from several sections and several years of the undergraduate engineering programme.

3.2 Study Population and Sampling

The target population comprised undergraduate engineering students as well as master's and PhD degree holders. Second-, third- and fourth-year students were recruited through convenience sampling and were given the questionnaire. Of 195 responses received, 9 came from respondents who were not B. Tech students and were excluded, leaving a final analytic sample of $N = 186$. The sample consisted of 116 women (62.4%) and 70 men (37.6%), spread across II Year ($n = 38$, 20.4%), III Year ($n = 89$, 47.8%) and IV Year ($n = 59$, 31.7%).

3.3 Instrument Design and Constructs

The questionnaire had two parts. Part A collected demographic and usage information: gender, year of study, average daily Internet use in hours, the devices used to go online, whether the respondent had ever attended a cyber security course or workshop, and whether they had personally experienced a cyber attack. Part B comprised 56 statements rated on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree), grouped into 10 theory-derived constructs, as listed in Table 1.

Construct	Theoretical Basis	Items	α
Knowledge / Awareness (KA)	Cybersecurity literacy	8	0.89
Perceived Severity (PS)	PMT – Threat appraisal	5	0.83
Perceived Susceptibility (PSU)	PMT – Threat appraisal	5	0.82
Perceived Benefits (PBN)	PMT – Coping appraisal	5	0.88
Self-Efficacy (SE)	PMT – Coping appraisal	5	0.89
Perceived Usefulness (PU)	TAM	5	0.91
Perceived Ease of Use (PEOU)	TAM	5	0.91
Privacy Concern (PC)	Privacy calculus	3	0.83
Protective Behaviour (PB)	Behavioural outcome	10	0.93
Behavioural Intention (BI)	Behavioural outcome	5	0.89

Table 1. Study constructs, theoretical grounding, item count, and internal consistency (Cronbach's α)

3.4 Data Collection Procedure

At the start of the questionnaire, respondents were told that the study had an academic purpose and that their answers would be analysed only in anonymous, de-identified and aggregated form. Apart from an optional institutional e-mail address, which was not analysed, no personally identifying information was gathered. Data collection took place over several weeks during the 2026 academic year.

3.5 Data Cleaning

Before analysis, the raw export was cleaned systematically. The “Average Daily Internet Usage” question was answered in free text and produced highly varied responses. Entries that could not be read as a duration of use (for example “About nearly 4–5 hours”, “2 GB”, “1:05” and “Don’t know”) were recoded as missing, as were implausible values above 18 hours per day. The resulting Internet-usage variable covers 144 of the 186 respondents (range = 1–8 hours/day, $M = 4.94$ hours/day, $SD = 2.31$ hours/day). Multi-select answers in the “Device(s) Used” field were collapsed into three categories: Mobile, Laptop and Both. No Likert data were missing; all 186 retained respondents answered all 56 items.

3.6 Statistical Analysis

Each construct score was computed as the mean of its items. Internal consistency was assessed with Cronbach’s alpha for every scale and for the full 56-item instrument. Descriptive statistics (mean, standard deviation, minimum and maximum) were obtained for all constructs. Groups were compared with one-way ANOVA for year of study and Welch’s independent-samples t-test for gender, workshop attendance and prior cyber attack experience, taking $p < .05$ as the threshold for significance throughout. Pearson correlations were computed among all ten constructs. Two multiple linear regression models were then fitted, one with Protective Behaviour and one with Behavioural Intention as the outcome. In each, the other eight PMT/TAM antecedent constructs (Knowledge/Awareness, Perceived Severity, Perceived Susceptibility, Perceived Benefits, Self-Efficacy, Perceived Usefulness, Perceived Ease of Use and Privacy Concern) were entered simultaneously. All analyses were run in Python 3.12 using pandas, SciPy and statsmodels.

3.7 Ethical Considerations

The study followed standard ethical practice for low-risk, anonymous educational surveys. A description of the study was presented at the start of the questionnaire, and no questions were asked about personal, financial or health information. Completing the form was not compulsory, and respondents could leave at any point without submitting their answers.

4. RESULTS

4.1 Demographic and Usage Profile of Respondents

Of the 186 B. Tech respondents, 116 (62.4%) were female and 70 (37.6%) were male. By year of study, 20.4% were in II year, 47.8% in III year and 31.7% in IV year. For Internet access, 101 respondents (54.3%) used only a mobile phone, 81 (43.5%) used both a mobile phone and a laptop, and the remainder used only a laptop. Only 57 respondents (30.6%) reported having attended a cyber security course or workshop previously, whereas 128 (68.8%) had never done so. A small minority (18 respondents, 9.7%) had personally experienced a cyber attack; the large majority (90.3%) had not. Figure 1 summarises these demographic and usage characteristics.

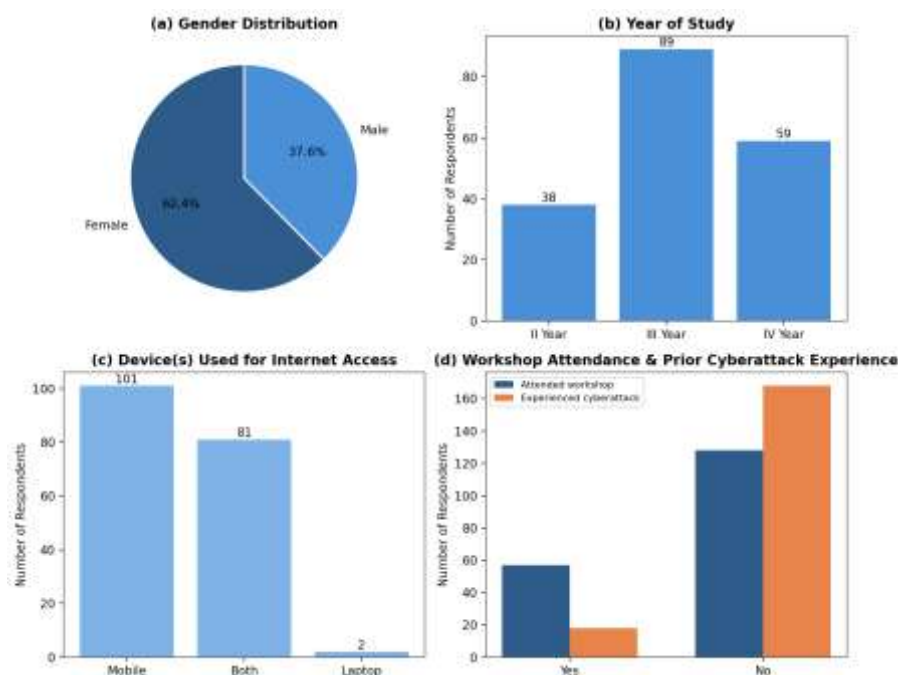


Figure 1. Demographic and usage profile of respondents (N = 186): (a) gender distribution; (b) year of study; (c) device(s) used for Internet access; (d) workshop attendance and prior cyber attack experience.

4.2 Reliability and Descriptive Analysis of Constructs

As Table 1 shows, alpha exceeded the conventional 0.70 benchmark for all ten constructs, ranging from $\alpha = 0.82$ (Perceived Susceptibility) to $\alpha = 0.93$ (Protective Behaviour), and the full 56-item scale reached an excellent $\alpha = 0.98$. Descriptive statistics for the ten constructs are given in Table 2 and plotted in Figure 2. Responses were generally favourable: every construct had a mean above the scale midpoint of 3.0. Perceived Benefits had the highest mean ($M = 3.89$, $SD = 0.73$), showing that students widely accepted the value of standard protective measures. Perceived Ease of Use had the lowest mean ($M = 3.61$, $SD = 0.81$), which suggests that although students valued security tools, they found them relatively hard to use. This usability gap bears directly on adoption and is taken up in Section 5.

Construct	M	SD	Min	Max	α
Knowledge/Awareness (KA)	3.67	0.73	1.0	5.0	0.89
Perceived Severity (PS)	3.75	0.72	1.4	5.0	0.83
Perceived Susceptibility (PSU)	3.62	0.70	1.2	5.0	0.82
Perceived Benefits (PBN)	3.89	0.73	1.8	5.0	0.88
Self-Efficacy (SE)	3.75	0.71	1.0	5.0	0.89
Perceived Usefulness (PU)	3.84	0.76	1.4	5.0	0.91
Perceived Ease of Use (PEOU)	3.61	0.81	1.0	5.0	0.91
Privacy Concern (PC)	3.69	0.83	1.0	5.0	0.83
Protective Behaviour (PB)	3.70	0.74	1.0	5.0	0.93
Behavioural Intention (BI)	3.69	0.83	1.0	5.0	0.89

Table 2. Descriptive statistics for study constructs (N = 186; 5-point Likert scale)

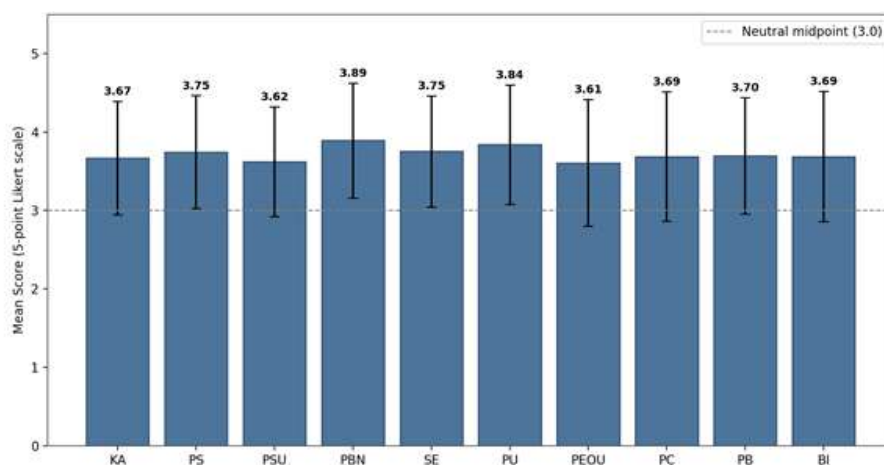


Figure 2. Mean scores ($\pm$ SD) across the ten study constructs.

4.3 Correlation Among Constructs

Pearson correlations among the ten constructs were all positive and moderate to strong, from $r = .54$ to $r = .79$ (Figure 3), and every pairwise correlation was significant at $p < .001$. Protective Behaviour was most strongly related to Perceived Ease of Use ($r = .79$) and Self-Efficacy ($r = .78$). Behavioural Intention was most strongly related to Protective Behaviour ($r = .77$) and Perceived Usefulness ($r = .72$), and Knowledge/Awareness to Protective Behaviour ($r = .69$) and Self-Efficacy ($r = .68$). This consistently positive pattern fits the idea, expected under the combined PMT–TAM framework, that the constructs form a coherent and interrelated behavioural system. The strong links of Self-Efficacy and Ease of Use with Behaviour also anticipate the regression results in Section 4.8.

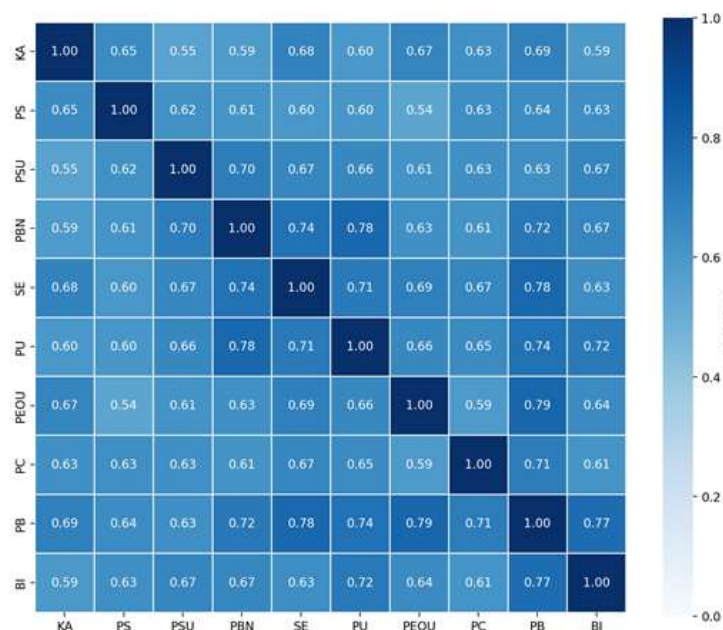


Figure 3. Pearson correlation matrix of the ten study constructs (all r significant at $p < .001$).

4.4 Differences by Gender

Welch's t -tests comparing male ($n = 70$) and female ($n = 116$) respondents (Figure 4) showed significantly higher scores for female students on four of the ten constructs: Perceived Benefits (Female $M = 3.99$ vs. Male $M = 3.73$; $t = -2.34$, $p = .021$), Perceived Usefulness (Female $M = 3.96$ vs. Male $M = 3.64$; $t = -2.63$, $p = .010$), Perceived Ease of Use (Female $M = 3.72$ vs. Male $M = 3.42$; $t = -2.38$, $p = .019$) and Behavioural Intention (Female $M = 3.86$ vs. Male $M = 3.41$; $t = -3.49$, $p = .001$).

The remaining constructs (Knowledge/Awareness, Perceived Severity, Perceived Susceptibility, Self-Efficacy, Privacy Concern and Protective Behaviour) did not differ significantly ($p > .05$), although Perceived Severity, Perceived Susceptibility and Protective Behaviour tended to be higher among women ($p = .06-.08$). $t = -2.34$, $p = .021$, Perceived Usefulness (Female $M = 3.96$ vs. Male $M = 3.64$; $t = -2.63$, $p = .010$), Perceived Ease of Use (Female $M = 3.72$ vs. Male $M = 3.42$; $t = -2.38$, $p = .019$), and Behavioural Intention (Female $M = 3.86$ vs. Male $M = 3.41$; $t = -3.49$, $p = .001$). Differences on the remaining constructs — including Knowledge/Awareness, Perceived Severity, Perceived Susceptibility, Self-Efficacy, Privacy Concern, and Protective Behaviour — did not reach conventional statistical significance ($p > .05$), although Perceived Severity, Perceived Susceptibility, and Protective Behaviour showed a consistent directional trend toward higher female scores ($p = .06-.08$).

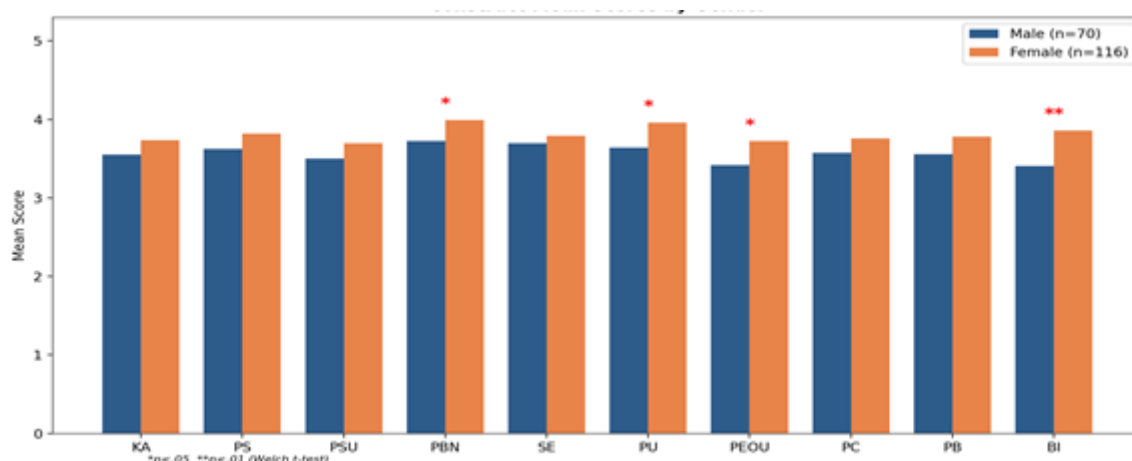


Figure 4. Construct mean scores by gender (Welch's t-test; * $p < .05$, ** $p < .01$).

4.5 Differences by Year of Study

One-way ANOVA across the II, III and IV Year cohorts found significant differences in Knowledge/Awareness ($F = 4.04$, $p = .019$), Perceived Severity ($F = 3.38$, $p = .036$), Perceived Susceptibility ($F = 6.05$, $p = .003$), Perceived Ease of Use ($F = 6.31$, $p = .002$), Privacy Concern ($F = 7.31$, $p = .001$) and Behavioural Intention ($F = 3.21$, $p = .043$). On these constructs, mean scores increased progressively from II Year to IV Year (e.g., Perceived Susceptibility: II Year $M = 3.28$, III Year $M = 3.69$, IV Year $M = 3.75$; Perceived Ease of Use: II Year $M = 3.22$, III Year $M = 3.65$, IV Year $M = 3.79$). This suggests that perceived risk, comfort with technology and intention to protect oneself grow as students advance through the programme, with greater seniority accompanying the rise. No significant year-of-study differences emerged for Self-Efficacy, Perceived Benefits, Perceived Usefulness or Protective Behaviour ($p > .05$).

4.6 Effect of Prior Cyber security Workshop or Course Attendance

Previous attendance at a cyber security course or workshop was the strongest demographic differentiator in this study (Figure 5). Students who had attended ($n = 57$) scored significantly higher than those who had not ($n = 128$) on all ten constructs without exception (all $p \leq .011$): Knowledge/Awareness (4.02 vs. 3.52, $t = 4.58$, $p < .001$), Perceived Severity (3.95 vs. 3.66, $p = .011$), Perceived Susceptibility (3.89 vs. 3.51, $p = .001$), Perceived Benefits (4.16 vs. 3.78, $p = .002$), Self-Efficacy (4.09 vs. 3.61, $p < .001$), Perceived Usefulness (4.10 vs. 3.73, $p = .003$), Perceived Ease of Use (3.95 vs. 3.46, $p < .001$), Privacy Concern (3.99 vs. 3.56, $p = .001$), Protective Behaviour (4.03 vs. 3.56, $p < .001$) and Behavioural Intention (4.02 vs. 3.54, $p < .001$). This consistent and robust pattern is direct empirical evidence that structured cyber security education improves not only declarative knowledge but also threat appraisal, coping appraisal, technology acceptance and actual protective behaviour.

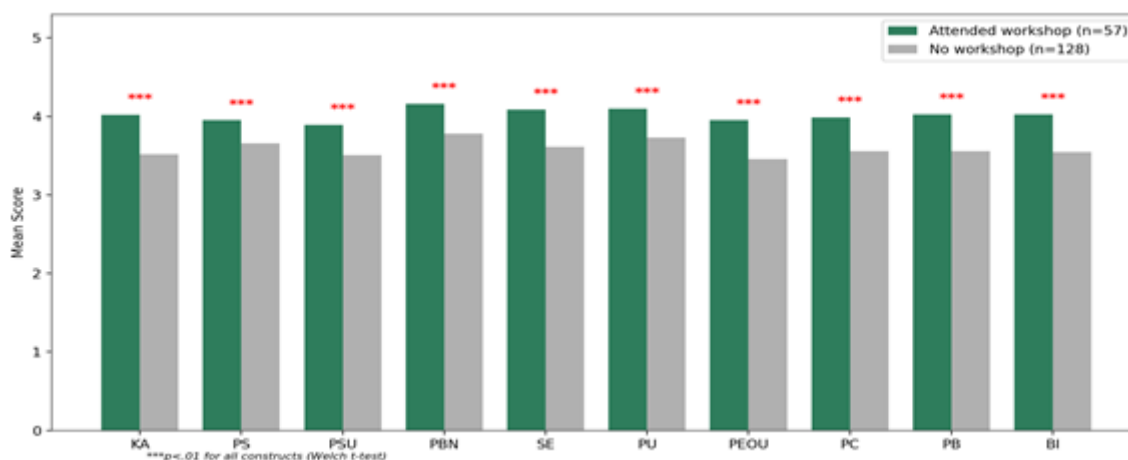


Figure 5. Construct mean scores by prior cyber security workshop/course attendance (** $p < .01$ for all constructs).

4.7 Effect of Prior Cyber attack Experience

Unlike workshop attendance, personal experience of a cyber attack ($n = 18$, 9.7% of the sample) was unrelated to any of the ten constructs (all $p > .18$). Students with a prior cyber attack had slightly higher Perceived Benefits (4.06 vs. 3.87) and slightly lower Perceived Usefulness (3.59 vs. 3.87) and Behavioural Intention (3.47 vs. 3.71) than those without, but none of these differences was statistically significant, most likely because the subgroup was small ($n = 18$). Daily Internet-usage hours were likewise not significantly correlated with any construct (all $|r| \leq .06$, $p > .45$), indicating that time online by itself is not a dependable indicator of cyber security awareness or behaviour in this sample.

4.8 Predictors of Protective Behaviour and Behavioural Intention

Two multiple linear regression models were fitted to determine the relative predictive strength of the eight antecedent constructs (Table 3; standardised coefficients are plotted in Figure 6). The model for Protective Behaviour was significant overall ($F(8, 177) = 78.95$, $p < .001$) and accounted for 78.1% of the variance ($R^2 = .781$, Adjusted $R^2 = .771$). Four predictors were significant: Self-Efficacy ($\beta = .237$, $p < .001$), Perceived Ease of Use ($\beta = .320$, $p < .001$), Perceived Usefulness ($\beta = .141$, $p = .023$) and Privacy Concern ($\beta = .150$, $p = .002$). Knowledge/Awareness, in contrast, was not an independent predictor of Protective Behaviour ($\beta = .042$, $p = .469$) once coping-appraisal and technology-acceptance constructs were controlled. This suggests that factual knowledge acts mainly indirectly, through its strong correlations with Self-Efficacy and Perceived Ease of Use (Section 4.3), rather than driving action directly.

The model for Behavioural Intention was likewise significant ($F(8, 177) = 37.74$, $p < .001$), explaining 63.0% of the variance ($R^2 = .630$, Adjusted $R^2 = .614$). Its significant predictors were Perceived Usefulness ($\beta = .332$, $p < .001$), Perceived Susceptibility ($\beta = .223$, $p = .010$), Perceived Severity ($\beta = .180$, $p = .025$) and Perceived Ease of Use ($\beta = .165$, $p = .027$). The contrast is informative for theory: actual Protective Behaviour was driven chiefly by coping-appraisal and usability constructs (a “can I do it, and is it easy?” logic), whereas Behavioural Intention depended more on threat appraisal and perceived usefulness (a “should I do it, and is it worth it?” logic). Threat-based messaging may therefore be better at building future intention, while interventions that improve usability and confidence may be better at turning intention into sustained everyday behaviour.

Predictor	β (PB)	p (PB)	β (BI)	p (BI)
Knowledge/Awareness (KA)	0.042	.469	0.055	.510
Perceived Severity (PS)	0.093	.090	0.180	.025 *
Perceived Susceptibility (PSU)	−0.086	.147	0.223	.010 *
Perceived Benefits (PBN)	0.097	.148	0.059	.547
Self-Efficacy (SE)	0.237	<.001 **	−0.025	.796

Predictor	β (PB)	p (PB)	β (BI)	p (BI)
Perceived Usefulness (PU)	0.141	.023 *	0.332	<.001 **
Perceived Ease of Use (PEOU)	0.320	<.001 **	0.165	.027 *
Privacy Concern (PC)	0.150	.002 **	0.057	.424
R ² / Adj. R ²	0.781 / 0.771		0.630 / 0.614	

Table 3. Regression models predicting Protective Behaviour and Behavioural Intention

Note. PB = Protective Behaviour; BI = Behavioural Intention. β = unstandardised OLS coefficient. * $p < .05$, ** $p < .01$. Both models $N = 186$; $DV = PB$: $F(8,177) = 78.95$, $p < .001$; $DV = BI$: $F(8,177) = 37.74$, $p < .001$.

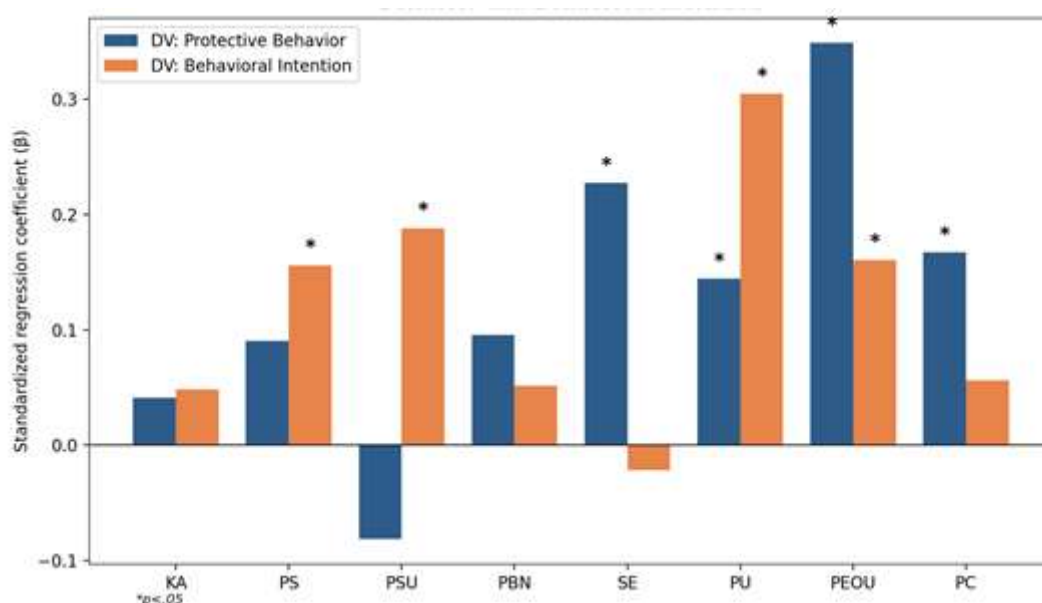


Figure 6. Standardised regression coefficients predicting Protective Behaviour and Behavioural Intention (* $p < .05$).

5. DISCUSSION

This study characterised cyber security awareness and digital privacy behaviour among Indian B. Tech engineering students through an integrated PMT–TAM framework and identified the psychological antecedents that best predict protective action. Three findings deserve discussion.

First, all ten constructs had moderately positive means above the scale midpoint, in line with earlier Indian and international findings that engineering and other technically oriented students report above-average baseline awareness (Senthilkumar & Easwaramoorthy, 2017; Pósa & Grossklags, 2022). Perceived Ease of Use had the lowest mean of the ten constructs ($M = 3.61$), reflecting a pattern common in TAM-based cyber security research: students may recognise that a security practice is desirable without finding it easy to carry out (Davis, 1989). The gap matters because Perceived Ease of Use was the strongest regression predictor of actual Protective Behaviour ($\beta = .320$), ahead of both Self-Efficacy and Knowledge. Institutional efforts that only raise threat awareness, without also simplifying the practical use of multi-factor authentication, password managers and privacy settings, are therefore likely to deliver diminishing behavioural returns. parallel effort to simplify the practical experience of using multi-factor authentication, password managers, and privacy settings, are likely to yield diminishing behavioural returns.

Second, Knowledge/Awareness did not independently predict Protective Behaviour once coping-appraisal and technology-acceptance constructs were controlled. This matches the well-documented “awareness–behaviour gap” in the wider information-security literature (Parsons et al., 2014; Rohan et al., 2023). At the bivariate level, knowledge was still strongly

correlated with Self-Efficacy ($r = .68$) and Protective Behaviour ($r = .69$). Knowledge thus appears to be a necessary foundation whose effect on behaviour is indirect: it builds confidence (self-efficacy) and perceived usability, which in turn drive action, rather than leading to behaviour by itself. The result agrees with Khan et al. (2023) and Han et al. (2025), who both found self-efficacy to be the leading PMT antecedent of cyber security behavioural outcomes in student populations.

Third, students who had previously attended a cyber security workshop or course held a consistent and sizeable advantage, scoring significantly higher on all ten constructs; Knowledge/Awareness alone rose from $M = 3.52$ to $M = 4.02$. This offers strong and coherent support for formal training and corroborates the experimental and quasi-experimental results of Khan et al. (2023) and Antunes et al. (2021). Since only 30.6% of the sample had received such training, the finding also points to a considerable unmet curricular need: most of the B. Tech students surveyed had never had structured cyber security instruction, even though they reported almost five hours of daily Internet use.

Female students scored significantly higher on Perceived Benefits, Perceived Usefulness, Perceived Ease of Use and Behavioural Intention. This differs somewhat from Bognár and Bottyán (2024), who found men scoring higher on proactive protection behaviours in a mainly Hungarian sample, but agrees with Kizilcec et al. (2023), who reported stronger privacy-related engagement among women in a five-country sample. Such divergence supports the view that gender effects in cyber security and privacy behaviour depend on the construct and context rather than being universal (García-Crespo et al., 2019), and the findings should not be generalised beyond the constructs and population examined here. The steady rise in Knowledge, Perceived Susceptibility, Perceived Ease of Use and Privacy Concern from II Year to IV Year fits a cumulative-exposure explanation, in which additional years of coursework, platform use and general maturity plausibly raise both risk perception and comfort with technology, although the cross-sectional design cannot exclude cohort effects.

6. CONCLUSION AND FUTURE WORK

This study investigated cyber security awareness and digital privacy behaviour among 186 Indian B.Tech engineering students using a ten-construct instrument that integrates Protection Motivation Theory and the Technology Acceptance Model. Reliability was good to excellent and mean scores were moderately positive, but knowledge alone did not significantly predict protective behaviour once self-efficacy, perceived ease of use, perceived usefulness and privacy concern were taken into account; the predictors jointly explained 78% of the variance in protective behaviour and 63% of the variance in behavioural intention. Students who had attended a structured cyber security workshop scored significantly higher on every construct, yet fewer than one-third of the sample had had such training. Indian engineering curricula would therefore gain most from hands-on, usability-focused instruction that builds self-efficacy, rather than from knowledge transmission alone. Future studies should extend the framework to multi-institutional samples with a better gender balance, use longitudinal or pre-post experimental designs to test whether training causes the observed differences, and check self-reported behaviour against objective measures such as password-manager adoption or click-through rates in simulated phishing.

ACKNOWLEDGEMENTS

Lorem ipsum dolor sit amet, consectetur adipiscing elit. The authors acknowledge the technical assistance provided by the Department of Natural Resources.

AUTHOR CONTRIBUTIONS

V. Harshavardhan: Conceptualization, Investigation, Writing.

C. Rani: Methodology, Analysis, Supervision.

J S Ananda Kumar: Formal Analysis, Review & Editing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

ETHICS STATEMENT

Ethical approval was not required for this study.

DATA AVAILABILITY STATEMENT

Data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

- [1] Alqahtani, M. A. (2022a). Cybersecurity awareness based on software and e-mail security with statistical analysis. *Computational Intelligence and Neuroscience*, 2022, Article 6775980. <https://doi.org/10.1155/2022/6775980>
- [2] Alqahtani, M. A. (2022b). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), Article 2589. <https://doi.org/10.3390/app12052589>
- [3] Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviors in school context. *Applied Sciences*, 11(23), Article 11269. <https://doi.org/10.3390/app112311269>
- [4] Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, 14(6), Article 588. <https://doi.org/10.3390/educsci14060588>
- [5] Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication*, 20, 133–155. <https://doi.org/10.23962/10539/23572>
- [6] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- [7] García-Crespo, Á., García, F., Therón, R., & García, J. (2019). Gender and Internet security: A study of Internet security habits and awareness of female and male users. *Computers in Human Behavior*, 95, 86–96. <https://doi.org/10.1016/j.chb.2019.01.023>
- [8] Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: Evidence from China. *Frontiers in Public Health*, 13, Article 1677024. <https://doi.org/10.3389/fpubh.2025.1677024>
- [9] Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, 125, Article 103049. <https://doi.org/10.1016/j.cose.2022.103049>
- [10] Kizilcec, R. F., Viberg, O., Jivet, I., Martínez Monés, A., Oh, A., Hrastinski, S., Mutimukwe, C., & Scheffel, M. (2023). The role of gender in students' privacy concerns about learning analytics: Evidence from five countries. In *LAK23: 13th International Learning Analytics and Knowledge Conference* (pp. 1–7). Association for Computing Machinery. <https://doi.org/10.1145/3576050.3576142>
- [11] Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, 18(8), 67–89. <https://doi.org/10.12700/aph.18.8.2021.8.4>
- [12] National Crime Records Bureau. (2025). Crime in India 2024. Ministry of Home Affairs, Government of India.
- [13] 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. <https://doi.org/10.1016/j.cose.2013.12.003>
- [14] Pósa, T., & Grossklags, J. (2022). Work experience as a factor in cyber-security risk awareness: A survey study with university students. *Journal of Cybersecurity and Privacy*, 2(3), 490–515. <https://doi.org/10.3390/jcp2030025>
- [15] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- [16] Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, 9(3), Article e14234. <https://doi.org/10.1016/j.heliyon.2023.e14234>
- [17] Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*, 263, Article 042043. <https://doi.org/10.1088/1757-899X/263/4/042043>
- [18] Trunkos, J. (2025). Examining the cybersecurity awareness of post-secondary students. *Issues in Information Systems*, 26(3), 149–157.