

Password Management Behaviors and Awareness Levels among Public Sector Employees in Trincomalee District, Sri Lanka

M.H.M. Humaidh^[1]

University of Vavuniya, Sri Lanka
haameemhumaidh@gmail.com

N.F. Zamla^[2]

University of Vavuniya, Sri Lanka
nifrazamla@gmail.com

Abstract

The public sector in Sri Lanka is undergoing a major digital transition. This change makes robust cybersecurity practices more important. Passwords are still the most common way to authenticate users. As a result, they are also one of the most exploitable weaknesses. This study looked at password management behaviors and cybersecurity awareness among public sector employees in the Trincomalee District in Sri Lanka. The study was guided by protection motivation theory. This theory includes threat appraisal and coping appraisal. Threat appraisal covers perceived severity and perceived susceptibility. Coping appraisal covers self-efficacy, response efficacy, and response cost. A structured questionnaire was given to 200 employees. These employees were selected through stratified random sampling. Statistical analysis was done using Pearson correlation and multiple linear regression. The results showed a consistent gap between policy requirements and actual employee behavior. Routine practices that are enforced by the organization were generally followed. One example is regular password changes. However, personally initiated behaviors were significantly weaker. These included avoiding password reuse and avoiding password sharing. Cybersecurity training was the strongest predictor of good password management behavior. Its beta value was 0.302. General cybersecurity awareness was the next strongest predictor with a beta of 0.290. Behavioral intention followed with a beta of 0.161. Organizational policy awareness had a beta of 0.141. Together, these predictors explained 71.7 percent of the variance in password management behavior. The R-squared value was 0.717. The findings show that effective cybersecurity requires more than policy mandates. It also requires practical, skills-based training. Such training enhances both employee competence and confidence. The implications for policymakers and public sector administrators are discussed.

Keywords: *Password management, Cybersecurity awareness, public sector employees, Protection Motivation Theory, Trincomalee*

JEL Codes: H83, O33, M15

1. INTRODUCTION

The rapid digitization of government services around the world has increased both the opportunities and the risks related to public sector information management. In Sri Lanka, this change is especially clear. The government is actively moving administrative services and citizen-facing services to online platforms. This type of digitization improves accessibility and operational efficiency. At the same time, it exposes sensitive government data to a growing number of cybersecurity threats. Passwords have been criticized for many years. However, they remain the main authentication mechanism across most public sector systems. The security of passwords is therefore a fundamental line of defense. It helps protect citizen data and institutional integrity.

The problem is not the existence of password policies. The problem is the adoption of those policies. Extensive international research shows a persistent gap. This gap exists between what organizational policies require and what employees actually do. Fitri and Yazid studied this in 2025. Vance, Siponen, and Pahlila studied it in 2012. Common failure modes include the use of weak passwords. These passwords are easy to guess. Another failure mode is credential reuse across multiple accounts. A third failure mode is informal password sharing among colleagues. These behaviors continue even among employees who are broadly aware of security requirements. In Sri Lanka, the National Cyber Security Strategy for 2025 to 2029 identifies human factor vulnerabilities as a priority concern. However, the extent to which this strategy leads to changed employee behavior at the district level remains largely uninvestigated. This study addresses that gap. It does so by examining password management behaviors and cybersecurity awareness levels. The participants are public sector employees in the Trincomalee District. The district is a strategically significant context. It is also under-researched. The district hosts a range of government departments. It has a diverse workforce. It is a focus area for national development initiatives. No prior academic study has systematically assessed cybersecurity behaviors among public servants at this district level.

The study makes two distinct contributions. The first contribution is theoretical. It extends the application of Protection Motivation Theory to the specific context of password management. This application takes place in a developing country's public sector setting. It tests whether the threat appraisal and coping appraisal constructs of protection motivation theory can adequately explain observed behavioral variance. The second contribution is practical. It generates district-level evidence. This evidence can guide the design of targeted training programs and policy interventions for public sector administrators in Sri Lanka.

The paper is organized as follows. Section 2 reviews the relevant literature. Section 3 presents the theoretical framework and research hypotheses. Section 4 describes the methodology. Section 5 presents the findings. Section 6 discusses the findings. Section 7 notes limitations and future directions. Section 8 concludes.

2. LITERATURE REVIEW

2.1 Password Security in the Digital Age

Passwords remain the most widely used authentication mechanism. They serve as the primary barrier between unauthorized actors and sensitive information. Their dominance is also a source of systemic vulnerability. Foundational work by Santhi Jeslet, Sivaraman, Uma, Thangadurai, and Punithavalli in 2010 established this. User comprehension and compliance with sound password protocols represent a persistently weak point in organizational defenses. Weak practices include the creation of simplistic passwords. These passwords are easy to guess. Another weak practice is credential reuse across services. A third weak practice is infrequent updates. These practices create vectors that malicious actors readily exploit. They use phishing, brute force attacks, and credential stuffing. This frequently leads to large-scale data breaches and unauthorized access events.

The organizational and societal consequences of such failures extend beyond immediate operational disruption. Public sector institutions bear a particular responsibility. Breaches that involve citizen data can erode public trust. They can also incur legal liability. They can undermine the legitimacy of digital government services. Sri Lanka is accelerating its e government agenda. Addressing human factor vulnerabilities has shifted from a technical concern to an essential governance imperative. This is stated in the National Cyber Security Strategy of Sri Lanka 2025 to 2029. It is also stated in the Cybersecurity Policy for Government Organizations by SLCERT in 2021.

2.2 Password Management and Awareness: Global and Organizational Perspectives

The policy practice gap in password security is well documented across organizational settings. Fitri and Yazid conducted a study of government employees in 2025. They found that even when comprehensive password policies are in place, employees frequently regard compliance as inconvenient. Employees then engage in workaroud behaviors. These behaviors prioritize ease of use over security. This disconnect highlights a fundamental insight. Effective cybersecurity cannot be achieved through policy creation alone. It is equally dependent on understanding and addressing the human factors that govern policy adoption.

A growing body of research supports security awareness training programs. These programs are a primary intervention. Security awareness training aims to give employees practical knowledge. This knowledge covers cyber threats and secure protocols. It helps change their role. They move from being a potential security liability to becoming an active human firewall. This is stated in sources from Proofpoint in 2024 and KnowBe4 in 2024.

The literature identifies several evidence-based strategies. These strategies support this transformation. One strategy is the use of password managers. Password managers ease the burden of creating and storing complex credentials. Another strategy is the use of multifactor authentication. This is a standard safeguard. A third strategy is the delivery of sustained and interactive training. This training goes beyond annual compliance exercises. These strategies are discussed in Abuzaraida and Zeki in 2020 and Verkijika in 2019. There is broad scholarly consensus on this point. Continuous education is essential. It helps cultivate a durable cybersecurity culture. This applies at the individual level. It also applies at the organizational level.

2.3 The Sri Lankan Context and Trincomalee District

Sri Lanka has made a commitment to digital government. This has made cybersecurity a national policy priority. The National Cyber Security Strategy for 2025 to 2029 provides a formal framework. The Cybersecurity Policy for Government Organizations from SLCERT in 2021 also provides a formal framework. These frameworks aim to strengthen public sector digital defenses. Despite these policy developments, local analyses show that government websites and digital infrastructure still have exploitable vulnerabilities. This suggests a gap between strategic intent and ground level implementation. This gap is noted in sources such as Bulathgama in 2023.

National employment statistics show a substantial and diverse public sector workforce. This is documented by the Department of Census and Statistics in 2025. However, academic literature on the cybersecurity behaviors of public servants at the district level remains sparse. The Trincomalee District is recognized for its administrative importance. It is also recognized for its socio-economic diversity. This district offers an appropriate context for such an investigation. It has not been studied before in this way.

2.4 Research Gap and Hypotheses

A synthesis of the literature reveals three core findings. The first finding is that password security remains a critically weak component of organizational cybersecurity. This is driven primarily by inconsistent human behavior. This is noted in the work of Santhi Jeslet and colleagues in 2010, Fitri and Yazid in 2025, and Ifinedo in 2012. The second finding is that a well-documented gap persists between policy prescription and employee practice. This gap can be meaningfully reduced through targeted awareness and training. This is discussed in Vance and colleagues in 2012 and Ng in 2020. The third finding is that despite a national policy framework, empirical evidence on the effectiveness of cybersecurity implementation at the district level in Sri Lanka is absent.

From this gap, the following research hypotheses are advanced:

- H1:** Cybersecurity awareness is positively associated with password management behaviour.
- H2:** Organisational policy awareness and enforcement are positively associated with password management behaviour.
- H3:** Cybersecurity training exposure and effectiveness are positively associated with password management behaviour.
- H4:** Behavioural intention to comply with security practices is positively associated with password management behaviour.

3. THEORETICAL FRAMEWORK

3.1 Protection Motivation Theory

This study uses protection motivation theory as its primary theoretical lens. Protection Motivation Theory is often shortened to PMT. It was first proposed by Rogers in 1975. It was later refined for cybersecurity contexts. Johnston and Warkentin did this in 2010. Herath and Rao also did this in 2009. PMT offers an empirically validated framework. It helps explain when and why individuals adopt protective behaviors. These behaviors are adopted in response to perceived threats. This makes the theory well suited for analyzing password management decisions.

Protection Motivation Theory is used in this study. It is often called PMT. The theory proposes that an individual's decision to engage in a protective behavior is determined by two cognitive appraisal processes. These processes happen in parallel. The first process is threat appraisal. Threat appraisal evaluates the perceived severity of a potential harm. It also evaluates the individual's perceived susceptibility to that harm. When both severity and susceptibility are perceived as high, the individual is motivated to take protective action. The second process is coping appraisal. Coping appraisal evaluates three things. It evaluates whether the recommended protective behavior is effective. This is called response efficacy. It evaluates whether the individual is capable of performing the behavior. This is called self-efficacy. It also evaluates how costly or burdensome compliance would be. This is called response cost. Protective motivation and the resulting behavioral intention are maximized when threat appraisal is high and coping appraisal is favorable. Low threat appraisal leads to complacency. Poor coping appraisal leads to perceived helplessness or excessive burden. Either of these inhibits protective behavior. This happens even among individuals who are nominally aware of security requirements. This explanation is based on Floyd, Prentice Dunn, and Rogers from 2000.

3.2 PMT Applied to Password Behavior

In this study, threat appraisal is defined in a specific way. It is defined through employee perceptions. These perceptions are about the likelihood of account compromise. They are also about the consequences of account compromise. Employees who believe their accounts are unlikely targets are considered low-threat appraisers. Employees who see breaches as inconsequential are also considered low-threat appraisers. These employees are expected to have weaker password practices. Coping appraisal is defined in a specific way as well. It is defined through three factors. The first factor is self-efficacy. This is confidence in one's ability to create and manage strong passwords. The second factor is response efficacy. This is the belief that strong passwords meaningfully reduce risk. The third factor is response cost. This is the perceived difficulty of complying with password requirements. Employees with low coping appraisal are those who feel unable to manage passwords effectively. They may also find compliance burdensome. These employees are also expected to demonstrate poor password hygiene.

The study measures four independent variables. These variables are cybersecurity awareness, organizational policy awareness, training exposure and effectiveness, and behavioral intention. These four variables map directly onto the constructs of protection motivation theory. Cybersecurity awareness and policy awareness both inform threat appraisal. Training and

behavioral intention primarily engage coping appraisal. They do this by building self-efficacy and reinforcing response efficacy. This explicit alignment allows the regression findings to be interpreted through a diagnostic lens based on protection motivation theory. It also enables targeted interventions.

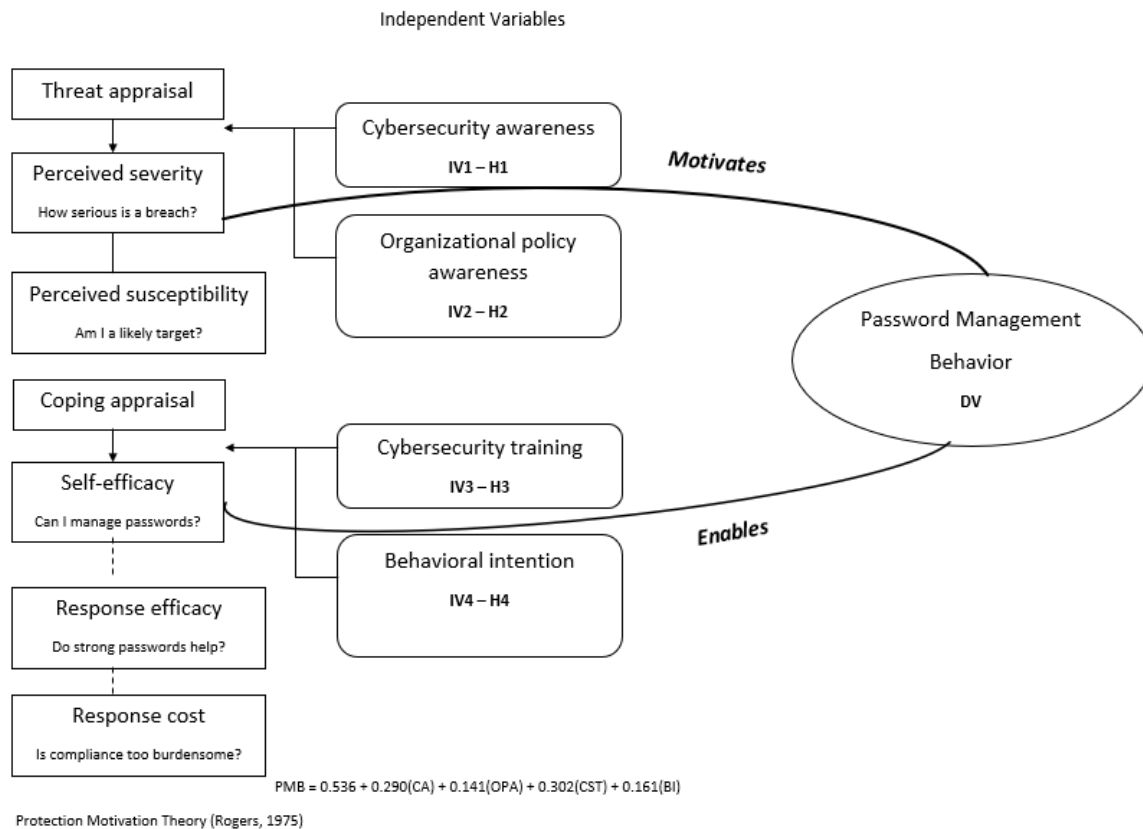


Figure 1. Conceptual Framework Based on Protection Motivation Theory)

4. RESEARCH METHODOLOGY

4.1 Research Design

A quantitative, cross-sectional survey design was used. This approach was chosen for its ability to measure and compare variables across a large sample. It can also identify statistical relationships between constructs. In this study, the constructs are the Protection Motivation Theory-related predictors and observed password management behavior. This is noted in Bryman from 2016. A structured questionnaire served as the only data collection tool.

4.2 Population, Sample, and Sampling Procedure

The target population was all public sector employees in the Trincomalee District. This included administrative, technical, clerical, and managerial roles across government departments. A stratified random sampling technique was used. This technique ensured representative coverage. Departments were first stratified by functional type. The functional types were administration, technical and IT services, clerical, and managerial. A random selection of employees was drawn from each stratum. The selection was done proportionally. This two-stage procedure minimized selection bias. It also ensured that the sample reflected the occupational diversity of the population. A total of 200 completed and valid responses were obtained. These responses were used for analysis.

4.3 Data Collection Instrument

The questionnaire was developed specifically for this study, anchored in PMT constructs (Rogers, 1975) and drawing on validated scales from prior information security behavior research. It comprised two sections. Section A collected demographic information: age, gender, highest educational qualification, job category, and years of public sector service. Section B contained 25 Likert-scale items (1 = Strongly Disagree to 5 = Strongly Agree) distributed equally across five constructs.

The dependent variable was password management behavior. This was shortened to PMB. It was measured using five items. These items assessed password uniqueness, change frequency, complexity, secure storage, and non-sharing practices. There were four independent variables. The first independent variable was cybersecurity awareness. It was measured with five items. These items gauged knowledge of password characteristics and threats such as phishing and social engineering. The second independent variable was organizational policy awareness and enforcement. It was measured with five items. These items measured perceived clarity and active enforcement of password policies. The third independent variable was training exposure and effectiveness. It was measured with five items. These items evaluated the frequency and perceived utility of cybersecurity training. The fourth independent variable was behavioral intention. It was measured with five items. These items assessed motivation to adopt and sustain stronger password practices. Sample items and prior sources are presented in Table 1.

The instrument was pilot tested before full deployment. A total of 15 public sector employees took part in the pilot test. Minor changes were made to the wording based on feedback from the pilot. For the final distribution, two channels were used. One channel was digital through Google Forms. The other channel was physical paper forms. This approach was used to reach employees across different departments. Participation was voluntary and anonymous. No personally identifiable information was collected. This satisfied the ethical requirement for confidentiality.

Table 1. Measurement of Variables and Source Instruments

Variable	Construct Definition	Sources	Measurement
Password Management Behaviour (DV)	Consistent application of recommended practices in creating, storing, and updating passwords for work accounts.	Santhi Jeslet et al. (2010); Fitri & Yazid (2025)	5-point Likert scale (1 = Strongly Disagree; 5 = Strongly Agree)
Cybersecurity Awareness (IV1)	Individual knowledge and recognition of password-related threats, best practices, and potential breach consequences.	Abuzaraida & Zeki (2020); Verkijika (2019)	5-point Likert scale
Organisational Policy Awareness & Enforcement (IV2)	Employee perception of the existence, clarity, and active enforcement of cybersecurity and password policies.	Fitri & Yazid (2025); Herath & Rao (2009)	5-point Likert scale
Training Exposure & Effectiveness (IV3)	Prior participation in, and perceived usefulness of, formal cybersecurity training provided by the organisation.	Vance et al. (2012); Ng (2020)	5-point Likert scale
Behavioural Intention (IV4)	Self-reported motivation and planned actions	Ajzen (1991); Ifinedo (2012)	5-point Likert scale

toward adopting stronger
password management
practices.

4.4 Data Analysis

Data were analyzed using SPSS Version 26. The analysis proceeded in three stages. In the first stage, descriptive statistics were calculated. These included frequencies, percentages, means, and standard deviations. They were used to profile the sample and summarize responses to all scale items. In the second stage, Pearson correlation analysis was conducted. This was done to examine the strength and direction of bivariate relationships. The relationships between each independent variable and the dependent variable were assessed. In the third stage, multiple linear regression analysis was performed. This assessed the collective and individual predictive power of the four independent variables on password management behavior. The significance threshold was set at p less than .05 throughout.

5. RESULTS

Table 2. Demographic Profile of Respondents

	Frequency	Percent (%)
Age Group		
Under 30	40	20.0
30–40	70	35.0
41–50	50	25.0
Above 50	40	20.0
Gender		
Male	110	55.0
Female	86	43.0
Prefer not to say	4	2.0
Qualification		
G.C.E. (O/L)	40	20.0
G.C.E. (A/L)	56	28.0
Diploma	44	22.0
Bachelor's Degree	40	20.0
Postgraduate	14	7.0
Other	6	3.0

Job Category		
Administrative	60	30.0
Technical/IT	30	15.0
Clerical	70	35.0
Managerial	20	10.0
Other	20	10.0
Years of Service		
Less than 1 year	10	5.0
1–3 years	30	15.0
4–7 years	40	20.0
8–15 years	60	30.0
More than 16 years	60	30.0

Table 2 summarizes the demographic profile of the stratified representative sample of 200 public sector employees within the Trincomalee District. The age profile reflects a mature workforce, with a plurality of respondents (35%) aged 30–40, followed by 25% in the 41–50 cohort. Both early-career (under 30) and senior (above 50) participants are equally represented at 20% each. Gender composition indicates a slight male majority at 55%, while female respondents constitute 43%, with a negligible 2% non-disclosure rate. Educational attainment within the sample is diverse: while 28% hold G.C.E. Advanced Level qualifications, nearly half the sample (49%) hold tertiary qualifications, including diplomas (22%), bachelor's degrees (20%), and postgraduate degrees (7%). Professionally, the cohort is anchored by clerical (35%) and administrative (30%) personnel, supplemented by technical/IT (15%) and managerial (10%) staff. Notably, 60% of respondents have eight or more years of service, with 30% exceeding sixteen years of tenure.

5.2 Reliability Analysis

Internal consistency was assessed using Cronbach's alpha. This was done for each scale. It was also done for the combined instrument. All values exceeded the conventional threshold of 0.70. This threshold was recommended by Hair, Black, Babin, and Anderson in 2019. Table 3 summarizes the results. The dependent variable scale for password management behavior had an alpha of 0.746. The individual independent variable scales had alphas ranging from 0.742 to 0.804. The training scale had an alpha of 0.742. The cybersecurity awareness scale had an alpha of 0.804. These values indicate good to very good reliability. The overall instrument had an alpha of 0.942 across all 25 items. This confirms excellent internal consistency.

Table 3. Cronbach's Alpha Reliability Coefficients (N = 200)

Scale	No. of Items	Cronbach's α	Interpretation
Password Management Behavior (DV)	5	0.746	Good
Cybersecurity Awareness (IV1)	5	0.804	Very Good
organizational Policy Awareness (IV2)	5	0.762	Good
Training Exposure & Effectiveness (IV3)	5	0.742	Good
Behavioral Intention (IV4)	5	0.757	Good
Full Instrument (all items)	25	0.942	Excellent

Note. Interpretation benchmarks based on Hair et al. (2019): ≥ 0.90 = Excellent; $0.80-0.89$ = Very Good; $0.70-0.79$ = Good.

5.3 Descriptive Statistics

Table 4 shows the means and standard deviations for the Password Management Behavior scale. The highest scoring item was regular password changing. This was done in line with recommended intervals. The mean was 4.03. The standard deviation was 0.98. This suggests that this institutionally mandated behavior is reasonably well embedded. The use of complex, mixed character passwords scored moderately high. The mean was 3.82. The standard deviation was 0.94. Avoidance of insecure storage methods also scored moderately high. The mean was 3.71. The standard deviation was 0.96. However, two items scored notably lower. The first was using unique passwords for different work accounts. The mean was 3.43. The standard deviation was 1.02. The second was refraining from sharing passwords with colleagues or family members. The mean was 3.17. The standard deviation was 1.01. The second item represents the weakest compliance point across the entire dependent variable scale. It also constitutes a significant security risk. Informal sharing may circumvent organizational controls.

Table 4. Descriptive Statistics - Password Management Behavior (DV)

Survey Item	N	Mean	SD
I regularly change my work-related passwords according to recommended intervals.	200	4.03	0.98
I use a combination of letters, numbers, and special characters to create strong passwords.	200	3.82	0.94
I avoid writing down my work passwords or storing them in unsecured places.	200	3.71	0.96
I use unique passwords for different work accounts.	200	3.43	1.02
I never share my work passwords with colleagues or family members.	200	3.17	1.01

For cybersecurity awareness, which was the first independent variable, respondents showed the strongest awareness of the consequences of password compromise. The mean for this item was 3.94. The standard deviation was 0.97. Respondents also felt reasonably confident recognizing suspicious login requests. The mean for this item was 3.81. The standard deviation was 0.95. However, knowledge of what specifically constitutes a strong password was only moderate. The mean for this item was 3.17. The standard deviation was 1.01. Understanding of phishing and social engineering tactics was the weakest item across the entire awareness scale. The mean for this item was 3.06. The standard deviation was 0.98. This pattern suggests that employees hold general awareness of risk. However, they lack the specific technical knowledge needed to counteract targeted attacks.

For organizational policy awareness and enforcement, which was the second independent variable, employees showed strong perceptions in two areas. They perceived active enforcement through mandatory updates and audits. The mean was 4.05. The standard deviation was 0.97. They also perceived management communication of password security importance. The mean was 3.91. The standard deviation was 0.96. However, awareness of a clearly written and accessible password policy was markedly lower. The mean was 3.02. The standard deviation was 0.98. This reveals a disconnect between perceived enforcement and documented policy clarity.

For Training Exposure and Effectiveness, which was the third independent variable, scores were moderate overall. Training materials were rated as clear and relevant. The mean was 3.62. The standard deviation was 0.99. Respondents expressed reasonable confidence in applying learned password practices. The mean was 3.51. The standard deviation was 1.02. Perceived improvement in ability to manage passwords was moderate. The mean was 3.34. The standard deviation was 1.03. Fewer respondents reported having received formal training within the preceding 24 months. The mean was 3.20. The standard deviation was 1.02. This suggests inconsistency in training frequency.

For behavioral intention, which was the fourth independent variable, respondents expressed the strongest intention to update weak passwords imminently. The mean was 3.72. The standard deviation was 0.96. They also expressed a strong intention to report suspicious incidents. The mean was 3.54. The standard deviation was 1.01. Motivation dropped considerably when compliance required extra effort. The mean was 3.15. The standard deviation was 1.01. This confirms that response cost is a meaningful barrier to behavioral follow-through.

5.4 Pearson Correlation Analysis

Table 5 shows the Pearson correlation matrix for all variables. All four independent variables were strongly correlated with the dependent variable. The correlations were positive. They were significant at the $p < .001$ level. This satisfies the assumption of meaningful bivariate associations. This is a prerequisite for regression analysis. Cybersecurity awareness had the highest correlation with password management behavior. The correlation was $r = .793$. Training was next with $r = .791$. Organizational policy awareness had $r = .751$. Behavioral Intention had $r = .739$. The intercorrelations among the independent variables were also substantial. They ranged from $r = .747$ to $.804$. This was expected. The variables have conceptual overlap under protection motivation theory. Multicollinearity was examined as part of the regression diagnostics.

Table 5. Pearson Correlation Matrix (N = 200)

Variable	1. PMB	2. CA	3. OPA	4. CST	5. BI
1. Password Management Behavior (PMB)	1.000	.793**	.751**	.791**	.739**
2. Cybersecurity Awareness (CA)	.793**	1.000	.800**	.804**	.747**
3. Organizational Policy Awareness (OPA)	.751**	.800**	1.000	.763**	.763**
4. Cybersecurity Training (CST)	.791**	.804**	.763**	1.000	.758**
5. Behavioral Intention (BI)	.739**	.747**	.763**	.758**	1.000

Note. ** $p < .001$ (two-tailed). PMB = Password Management Behavior; CA = Cybersecurity Awareness; OPA = Organizational Policy Awareness; CST = Cybersecurity Training; BI = Behavioral Intention.

5.5 Multiple Regression Analysis

Multiple linear regression was conducted with the four independent variables entered simultaneously (enter method) to predict password management behavior. Table 6 presents the model summary, and Table 7 the coefficients.

Table 6 . Regression Model Summary

Model	R	R ²	Adjusted R ²	SEE
1	.847	.717	.711	.372

Note. Predictors: Cybersecurity Awareness, Organizational Policy Awareness, Cybersecurity Training, Behavioral Intention. Dependent Variable: Password Management Behavior. SEE = Standard Error of the Estimate.

The model achieved a strong fit: $R = .847$, $R^2 = .717$, and adjusted $R^2 = .711$. Approximately 71.7% of the variance in password management behavior was explained by the four predictors, confirming the collective explanatory power of the PMT-derived model.

Table 7. Regression Coefficients

Variable	B	SE	β	t	Sig.
(Constant)	.536	.143		3.757	< .001
Cybersecurity Awareness (IV1)	.290	.071	.304	4.088	< .001
organizational Policy Awareness (IV2)	.141	.070	.144	2.026	.044
Cybersecurity Training (IV3)	.302	.069	.310	4.348	< .001
Behavioral Intention (IV4)	.161	.064	.166	2.515	.013

Note. Dependent Variable: Password Management Behavior. B = unstandardized coefficient; SE = standard error; β = standardized coefficient.

All four predictors were statistically significant at the $p < .05$ level. This indicates that each independently contributed to explaining password management behavior. This supports H1 through H4. Cybersecurity training was the strongest predictor. Its beta value was .310. Cybersecurity awareness was the next strongest predictor. Its beta value was .304. Behavioral intention was also significant. Its beta value was .166. Organizational policy awareness was significant as well. Its beta value was .144. These last two had smaller effect sizes. The regression equation is expressed as follows.

$$\text{PMB} = 0.536 + 0.290(\text{CA}) + 0.141(\text{OPA}) + 0.302(\text{CST}) + 0.161(\text{BI}) + \varepsilon$$

6. DISCUSSION

The findings provide a coherent and interpretable picture of password management behavior. This picture is drawn from the public sector in Trincomalee. It aligns closely with the Protection Motivation Theory framework. It also corroborates prior research on the policy practice gap in organizational cybersecurity.

The descriptive results map onto the Protection Motivation Theory diagnostic framework. This mapping is notably clear. Behaviors that are institutionally mandated and routinely enforced show relatively higher compliance. One example is changing passwords at specified intervals. The mean for this behavior was 4.03. This is consistent with the expectation that external enforcement partially compensates for low individual coping appraisal. However, behaviors that require personal initiative and internalized motivation show markedly lower adherence. Avoiding password reuse is one such behavior. The mean was 3.43. Refraining from sharing passwords is another. The mean was 3.17. This divergence between enforced and discretionary behaviors is a hallmark of low coping appraisal under protection motivation theory. It specifically points to low self-efficacy. Employees follow rules when they must. However, they do not sustain secure

practices when the choice is left to them.

The threat appraisal dimension shows a similar pattern. Employees have reasonable awareness of the consequences of a breach. The mean was 3.94. This corresponds to adequate severity perception. However, their understanding of specific attack vectors is notably weak. This includes understanding of phishing and social engineering. The mean was 3.06. This indicates low susceptibility perception. This configuration is high severity awareness but low susceptibility awareness. It is consistent with a distance bias. In this bias, individuals acknowledge that breaches are serious. However, they do not believe they personally are likely targets. Such biases are well documented in the Protection Motivation Theory literature. This is noted by Floyd and colleagues in 2000. These biases can suppress protective motivation. This can happen even when severity perceptions are adequate.

The regression results directly address the relative importance of interventions that align with protection motivation theory. Cybersecurity training was the strongest predictor of sound password behavior. Its beta value was .310. This finding is consistent with Vance and colleagues in 2012. They showed that training is the most effective way to enhance self-efficacy. Self-efficacy is the coping appraisal subcomponent most directly involved in behavioral follow-through. This finding has direct practical significance. It suggests that skill-building training does more than impart knowledge. It also builds the confidence needed to translate knowledge into consistent behavior. This confidence is self-efficacy. Cybersecurity awareness was nearly as strong a predictor. Its beta value was .304. This indicates that addressing threat appraisal deficits also meaningfully shifts behavior. This includes addressing susceptibility perceptions and knowledge of specific attack methods.

Organizational Policy Awareness had the weakest predictive effect among the significant predictors. Its beta value was .144. This finding complements the descriptive paradox noted earlier. Employees perceived strong enforcement. The mean for this item was 4.05. However, they reported poor awareness of a clearly articulated written policy. The mean for this item was 3.02. This suggests that current policy implementation is compliance-oriented rather than comprehension-oriented. Prior research identifies this pattern as a significant limitation of top-down security governance. This is noted in Fitri and Yazid in 2025. It is also noted in Herath and Rao in 2009. Policies appear to be enforced through system-level controls. They are not communicated as substantive guidance that employees can understand and internalize.

Behavioral Intention was significant. Its beta value was .166. However, it was moderated by response cost. When following guidelines required extra effort, intention scores dropped substantially. The mean for this item was 3.15. This is consistent with the response cost construct in protection motivation theory. It is also consistent with the broader behavioral economics literature on friction effects. People intend to behave securely. However, they do not follow through when compliance is burdensome. This finding has direct implications for tool provisioning. If organizations reduce the friction associated with secure password management, they can expect intention to translate more reliably into behavior. One way to reduce friction is through institutionally supported password managers.

7. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

This study has several limitations. These limitations should be considered when interpreting the findings. First, the study uses a cross-sectional design. This design captures attitudes and behaviors at a single point in time. It does not allow for causal inference. Longitudinal designs would be needed. Such designs would help establish whether changes in training or awareness produce corresponding changes in behavior over time. Second, the study relies exclusively on self-reported measures of password behavior. Social desirability bias may have inflated compliance estimates. Employees may report idealized practices rather than actual practices. Future research should complement survey data with behavioral audits. It could also use system-generated logs. This should be done where ethical and technical conditions permit.

Third, the sample is geographically restricted to the Trincomalee District. This focus allows for contextually specific insights. However, it limits direct generalization to other districts in Sri Lanka. It also limits generalization to public sectors in other countries. Comparative multi-district or national studies would help. Such studies would establish whether the patterns observed here are specific to Trincomalee. They would also show if the patterns are broadly representative of the public sector in Sri Lanka. Fourth, the study used convenience proximate stratified sampling. This approach was systematic. However, it may not fully account for all subgroups within the district public sector. This is particularly true for those in smaller or more remote departments. Finally, the study did not examine moderating variables. These include departmental cybersecurity culture. They also include IT infrastructure quality. Individual digital literacy is another moderating variable. All of these may meaningfully shape the relationships observed. Future research should include these contextual factors. This would help develop a more complete explanatory model.

8. CONCLUSION

This study investigated password management behaviors and cybersecurity awareness among public sector employees in the Trincomalee District of Sri Lanka. It used protection motivation theory as the guiding analytical framework. The results confirm a meaningful gap between policy-enforced compliance and self-directed secure behavior. Protection Motivation Theory attributes this gap primarily to deficits in coping appraisal. These deficits are low self-efficacy and elevated response cost perceptions. There is also inadequate susceptibility awareness on the threat appraisal side.

The regression analysis identified cybersecurity training as the strongest predictor of sound password management behavior. Cybersecurity awareness was the next strongest predictor. This is a significant finding for practice. It shows that practical, skills-oriented training is the most effective way to improve password hygiene in this population. Policy enforcement alone is not enough. Employees need information about what to do. They also need the practical skills and tools to do it consistently. They need the confidence that their efforts genuinely matter.

For policymakers and public sector administrators, these findings yield several actionable priorities. The first priority is investing in regular, practical cybersecurity training programs. These programs should build both skill and confidence. The second priority is addressing the specific susceptibility blind spots around phishing and social engineering. Current awareness efforts leave these blind spots unaddressed. The third priority is improving the accessibility and clarity of

written password policies. Organizations should not rely solely on system-level enforcement. The fourth priority is provisioning tools that reduce the effort cost of compliant behavior. Institutionally supported password managers are one example. Together, these measures can close the gap between policy intent and employee practice. This will strengthen the cybersecurity posture of Sri Lanka's digital government infrastructure at the district level.

REFERENCES

- Abuzaraida, M., & Zeki, A. (2020). Awareness and security issues in password management among Libyan university staff members. *International Journal of Advanced Research in Engineering and Technology*, 11(12), 1292–1303. <https://doi.org/10.34218/IJARET.11.12.2020.123>
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- AlHogail, A. (2021). Applying protection motivation theory to information security policy compliance in Saudi organisations. *Journal of Information Security and Applications*, 62, 103002. <https://doi.org/10.1016/j.jisa.2021.103002>
- Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.
- Bulathgama, T. (2023, January 10). Potential internet risks. Ministry of Defence, Sri Lanka.
- Cybersecurity Policy for Government Organizations. (2021, July). Sri Lanka Computer Emergency Response Team (SLCERT).
- Department of Census and Statistics. (2025). Census of public and semi-government sector employment – 2024: Preliminary report. Statistics Sri Lanka.
- Fitri, A., & Yazid, M. (2025). Improving password policy strategies: A government employee perspective. *Information and Computer Security*, 33(2), 1–25. <https://doi.org/10.1108/ICS-12-2024-0335>
- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407–429. <https://doi.org/10.1111/j.1559-1816.2000.tb02323.x>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95. <https://doi.org/10.1016/j.cose.2011.10.007>
- Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549–566. <https://doi.org/10.2307/20721433>

- KnowBe4. (2024). Security awareness training. <https://www.knowbe4.com/products/security-awareness-training>
- National Cyber Security Strategy of Sri Lanka 2025–2029. (2025). Cabinet Office Sri Lanka / CERT Sri Lanka.
- Ng, B. Y. (2020). The role of protection motivation theory in employees' information security policy compliance intentions. *Behaviour & Information Technology*, 39(9), 969–984. <https://doi.org/10.1080/0144929X.2019.1583280>
- NIST. (2017). Digital identity guidelines: Authentication and lifecycle management (NIST Special Publication 800-63B). National Institute of Standards and Technology.
- Proofpoint. (2024). What is security awareness training? Tools, FAQs, and more. <https://www.proofpoint.com/us/threat-reference/security-awareness-training>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Santhi Jeslet, D., Sivaraman, G., Uma, M., Thangadurai, K., & Punithavalli, M. (2010). Survey on awareness and security issues in password management strategies. *International Journal of Computer Science and Network Security*, 10(4), 1–7.
- Sri Lanka: Trincomalee in development discourse. (2012, August 3). Observer Research Foundation. <https://www.orfonline.org/research/sri-lanka-trincomalee-in-development-discourse>
- Vance, A., Siponen, M., & Pahnla, S. (2012). Motivating IS security compliance: The role of punishment and organisational policy. *Computers & Security*, 31(7), 891–903. <https://doi.org/10.1016/j.cose.2012.06.005>
- Verkijika, S. F. (2019). An affective model of software piracy. *Computers in Human Behavior*, 100, 112–119. <https://doi.org/10.1016/j.chb.2019.06.004>