Received: 25 April 2026 | Revised: 16 June 2026 | Accepted: 8 July 2026 | Published online: 4 August 2026

RESEARCH ARTICLE

Journal of Data Science and Intelligent Systems
2026, Vol. 00(00) 1–16
DOI: 10.47852/bonviewJDSIS620210144

BON VIEW PUBLISHING

An Integrated UTAUT, Machine Learning, and Association Rule Mining Analysis of Password Security Behavior Among Educational Personnel

Pita Jarupunphol[1,*] and Sujira Jeennoo[2]

[1] *Department of Digital Technology, Phuket Rajabhat University, Thailand*

[2] *Department of Digital Business Technology, Krabi Technical College, Thailand*

Abstract: This study examined password security behavior among educational personnel at Krabi Technical College using an integrated Unified Theory of Acceptanceand Use of Technology (UTAUT), machine learning, and association rule mining framework. Based on 210 survey responses and 50 variables, behavioral intention (BI) and use behavior (UB) were operationalized as composite scores derived from UTAUT-aligned Likert-scale items. In contrast, password behaviors captured practical routines such as password reuse, recovery capability, composition practices, and perceived attackability. Explanatory results showed that BI was mainly associated with hedonic motivation (β = 0.414), performance expectancy (β = 0.285), and facilitating conditions (β = 0.162), while UB was associated with BI (β = 0.444), habit (β = 0.206), and social influence (β = 0.142). Although the structural equation model indicated an excellent global fit, severe multicollinearity among constructs necessitated interpreting path coefficients as conditional associations rather than independent causal effects. Predictive analysis using five-fold cross-validation showed that construct-only ridge regression achieved the best performance for BI (RMSE = 0.491, R^2 = 0.650) and UB (RMSE = 0.553, R^2 = 0.640), with no statistically significant improvement over standard linear regression. Association rule mining revealed co-occurrence patterns centered on facilitating conditions, recovery capability, habit, and social influence. The findings support a parsimonious, interpretable approach to cybersecurity behavior analysis and provide actionable guidance for institutional password training, recovery support, and policy design.

Keywords: UTAUT, password security, behavioral intention, machine learning, association rule mining

1. Introduction

Password practices remain a foundational part of everyday cybersecurity behavior in educational organizations, yet insecure or inconsistent habits can persist even when users report generally positive attitudes toward digital security. Recent studies continue to show that cyber hygiene, password-management practices, and human cybersecurity behavior remain pressing problems across educational, organizational, and everyday digital contexts [1–5]. This tension makes password behavior a suitable setting for an integrated study that combines theoretical explanation with predictive assessment. A theory-only design can clarify why respondents report stronger behavioral intentions (BIs) or use behavior (UB), but it cannot, by itself, determine whether broader behavioral features improve out-of-sample prediction. Conversely, a prediction-only design may identify useful signals while offering weaker theoretical interpretation. The present study therefore treats explanation and prediction as related but distinct tasks [6–8].

Krabi Technical College provides a meaningful context for this analysis because password behavior is shaped not only by perceptions of usefulness and effort but also by habit, social context, recovery experience, and everyday account-management routines. Recent cybersecurity behavior and password-manager studies similarly emphasize that protective behavior depends on routines, coping appraisals, adoption decisions, and usability conditions rather than on awareness alone [9–15]. The available dataset includes both UTAUT-style survey items and practical password-behavior indicators, which support an integrated analytical design grounded in a partial UTAUT2 specification while allowing broader predictive comparison. It also includes multiple binary behavioral variables, making association rule mining (ARM) methodologically feasible as a complementary descriptive layer [16–18]. Although several extensions of the UTAUT model have been proposed, this study uses the term "UTAUT" as its primary reference framework.

***Corresponding author:** Pita Jarupunphol, Department of Digital Technology, Phuket Rajabhat University, Thailand. Email: p.jarupunphol@pkru.ac.th

The article is structured to avoid three common problems. First, statistical significance is not treated as evidence of predictive superiority. Second, predictive salience is not treated as proof of theoretical support. Third, association rules are not interpreted as causal mechanisms. Instead, each analytical stream is reported on its own terms and integrated only after the results have been established. This study addresses the following objectives:

1) To evaluate whether the available survey items support a defensible UTAUT explanation of password-related BI and UB.
2) To identify which constructs are most strongly associated with BI_score and UB_score in explanatory models.
3) To compare the predictive performance of theory-based, raw behavioral, and integrated-feature spaces using reproducible cross-validated machine learning.
4) To assess whether ARM reveals meaningful co-occurrence patterns that complement, rather than replace, theory and prediction.
5) To synthesize theoretical, predictive, and rule-based evidence into a publication-oriented interpretation of password security behavior in the institutional context.

This study contributes to cybersecurity behavior research in four ways. First, it integrates a UTAUT-based explanation, cross-validated machine learning, and ARM into a single analytical framework for understanding password security behavior among educational personnel. Second, it explicitly separates explanatory modeling, predictive modeling, and associative pattern discovery, thereby avoiding the common mistake of treating statistical significance, predictive accuracy, and co-occurrence rules as equivalent forms of evidence. Third, it evaluates whether construct-level theoretical representations outperform raw behavioral and integrated-feature spaces under reproducible five-fold cross-validation. Fourth, it translates ARM outputs into practical institutional recommendations for password-policy design, recovery support, cybersecurity training, and socially reinforced security routines.

The remainder of this article is structured as follows. Section 2 reviews UTAUT, password security behavior, machine learning in cybersecurity behavior research, and ARM. Section 3 presents the integrated analytical framework, dataset audit, construct mapping, explanatory modeling, predictive modeling, and ARM procedures. Section 4 reports the descriptive, explanatory, predictive, classification sensitivity, and ARM results. Section 5 discusses the theoretical, predictive, practical, and methodological implications, including limitations. Section 6 concludes the study and proposes future directions for research on institutional cybersecurity behavior.

2. Literature Review

Password security behavior remains a central issue in cybersecurity because authentication practices depend not only on technical requirements but also on user motivation, memory burden, habit, perceived usefulness, social norms, and institutional support. Recent studies show that password-management behavior is influenced by cybersecurity knowledge, perceived responsibility, usability constraints, password-manager adoption, memory anxiety, and coping appraisals. These findings suggest that password behavior should be studied as a socio-technical routine rather than as a purely technical compliance issue.

UTAUT and UTAUT2 provide a useful explanatory foundation by linking BI and technology use to performance expectancy (PE), effort expectancy (EE), social influence (SI), facilitating conditions (FC), hedonic motivation (HM), and habit (HB). In password security contexts, these constructs are relevant because users may adopt secure routines when they perceive security practices as useful, manageable, socially supported, easy to incorporate into routine practice, and compatible with everyday work. However, UTAUT alone may not capture practical password-management behaviors such as reuse, recovery capability, password composition, or perceived attackability. This limitation justifies combining UTAUT constructs with predictive modeling and ARM.

Machine learning has increasingly been used in cybersecurity behavior research to identify patterns that may not be fully captured by theory-based regression. Nevertheless, in survey-based cybersecurity datasets, larger and more flexible models do not always outperform interpretable linear or regularized models, especially when sample sizes are modest and predictors are highly correlated. For this reason, predictive models should be evaluated with cross-validation and interpreted separately from explanatory models. ARM adds a third perspective by identifying co-occurring behavioral states, such as whether high FC and recovery capability tend to co-occur with high SI or strong UB. These rules are useful for administrative interpretation, but they should not be treated as causal or temporal mechanisms.

2.1. UTAUT as the explanatory core

The theory-driven backbone of this study is a UTAUT specification. The dataset supports direct mapping for PE, EE, SI, FC, HM, HB, BI, and UB. This decision favors construct validity over nominal model completeness [16–24]. The theoretical logic is straightforward. BI is expected to reflect respondents' beliefs about usefulness, ease, support, social environment, enjoyment, and routine. UB should then depend partly on intention, while also reflecting direct enactment factors such as habit and enabling conditions. In a password security setting, these relationships are especially relevant because secure practice is rarely a one-time choice; it is a repeated behavior embedded in everyday digital work.

At the same time, password outcomes may also depend on concrete behavioral conditions not captured fully by theory scales alone, including password reuse, password composition, recovery capability, and change frequency. These variables justify the machine learning comparison and, when converted into transactional indicators, the ARM component. The integrated design therefore extends the UTAUT model without conflating theoretical constructs with auxiliary behavioral markers.

3. Proposed Methodology

3.1. The integrated analytical framework

The proposed integrated analytical framework is implemented as a four-stage, sequential pipeline that preserves a clear distinction between explanatory modeling, predictive modeling, and associative pattern discovery. The framework is illustrated below through a representative respondent profile to clarify the operational flow.

1) Step 1: data input and representation

A respondent completes a structured questionnaire consisting of UTAUT-aligned Likert-scale items (e.g., PE, HM, HB) alongside operational password-behavior indicators such as password reuse, recovery capability, and composition practices.

Likert-scale responses are aggregated into construct scores (e.g., BI_score and UB_score) using predefined item mappings. At the same time, behavioral indicators are retained either in their original binary form or discretized as needed for later analytical stages.

2) Step2: explanatory modeling (theory-driven analysis)

Construct scores derived in Step1 enter the explanatory modeling stage, where regression-based analyses are used to estimate conditional associations within the UTAUT framework. BI (BI_score) is modeled as a function of the core constructs. In contrast, UB (UB_score) is modeled using BI as a staged antecedent alongside additional constructs such as HB and SI. This stage focuses on interpretability and theoretical consistency rather than predictive optimization.

3) Step3: predictive modeling (out-of-sample generalization)

The same respondent is then included in the predictive modeling stage, in which multiple feature-space strategies, including construct-only features, raw behavioral features, and integrated representations, are evaluated using five-fold cross-validation. Linear, regularized, and classical machine learning models are compared based on generalization performance (e.g., RMSE and cross-validated R2), explicitly separating predictive accuracy from explanatory significance.

4) Step4: association rule mining (descriptive co-occurrence analysis)

Categorical representations of the respondent's attributes (e.g., high BI_score, recover_capable) are incorporated into ARM. This stage identifies stable co-occurrence patterns among constructs and behavioral indicators across respondents using support, confidence, and lift metrics. Importantly, these rules are interpreted strictly as descriptive associations rather than causal or temporal relationships. These steps demonstrate how a single dataset instance systematically flows through explanatory, predictive, and associative analyses without conflating their inferential purposes. This step-based framework reinforces the transparency, reproducibility, and methodological separation that motivate the proposed integrated design.

3.2. Data and audit

BI and UB were operationalized as composite scores from the survey instrument. BI_score was computed as the mean of the behavioral intention items, while UB_score was computed as the mean of the UB items. Other UTAUT-aligned construct scores were computed in the same way using their corresponding item groups. Practical password-behavior indicators were retained separately and included variables related to password reuse, password composition, recovery capability, number of passwords, perceived attackability, and related account-management practices. This design allowed the study to distinguish between psychological acceptance constructs and operational indicators of password behavior.

The raw dataset contained 210 rows and 50 columns, with no duplicates. Missingness was negligible: only EE2 contained one missing response (0.48%). The data combined demographics, password-behavior variables, and Likert-type indicators for the UTAUT-aligned constructs. Before any modeling, the dataset audit checked file structure, data types, missingness, outliers, categorical distributions, and suspicious patterns. The audit showed that most construct items were concentrated toward favorable responses, especially for PE, HB, BI, and UB. Several password-behavior variables were highly imbalanced, such as the near-universal use of numeric characters in passwords and the large share of respondents reporting more than one password. These patterns are analytically useful, but they also caution against overinterpreting rare subgroups.

3.3. Construct mapping and measurement quality

Construct mapping followed the observable item prefixes already present in the instrument: PE1–PE4, EE1–EE4, SI1–SI4, FC1–FC4, HM1–HM4, HB1–HB4, BI1–BI4, and UB1–UB4. Composite scores were then used for construct-level explanatory analysis and construct-only prediction. This mapping is defensible because the item groupings were directly represented in the data rather than inferred post hoc.

Table 1 summarizes internal consistency. All retained constructs achieved acceptable to excellent reliability, with Cronbach's alpha values ranging from 0.759 for HB to 0.958 for EE. This result supports construct aggregation, although the very high alpha for EE may also reflect strong item redundancy. The table indicates that measurement unreliability is unlikely to be the primary explanation for the weak effects observed in the regression stage. Instead, any nonsignificant construct effects should be interpreted more in terms of overlap among theoretically related constructs than in terms of poor scale quality.

Although the reliability values supported construct aggregation, very high reliability should not be interpreted as automatically superior measurement quality. High Cronbach's alpha may indicate that items are internally consistent, but extremely high values may also suggest item redundancy. In the present dataset, this issue is important because several UTAUT constructs were strongly correlated. Therefore, construct scores were retained for theoretical consistency and predictive parsimony, but coefficient-level interpretation was conducted cautiously and in conjunction with multicollinearity diagnostics.

Table 1
Reliability of retained construct scales

Construct	Alpha
Effort expectancy	0.958
Performance expectancy	0.904
Hedonic motivation	0.769
Behavioral intention	0.855
Use behavior	0.834
Social influence	0.918
Facilitating conditions	0.886
Habit	0.759

Note: Alpha = Cronbach's alpha. Higher values indicate stronger internal consistency, but very high values may also suggest item redundancy. Reliability results, therefore, support construct aggregation but should be interpreted together with the multicollinearity diagnostics.

3.4. Explanatory modeling

The explanatory equations and ARM metrics were grounded in standard statistical and data-mining formulations. The regression equations for BI_score and UB_score follow the general multiple-regression framework for estimating conditional associations among continuous composite variables. The machine

learning prediction equation follows the standard supervised learning formulation, while Root Mean Square Error (RMSE), Mean Absolute Error (MAE), and cross-validated R^2 are standard continuous-outcome performance metrics. The ARM metrics of support, confidence, and lift follow the classical ARM framework. The revised manuscript therefore cites the original or standard methodological sources when introducing these equations and metrics.

The explanatory stage used construct-level models for BI_score and UB_score. For BI, the predictors were EE_score, PE_score, HM_score, SI_score, FC_score, and HB_score. For UB, the same set of constructs was used, with BI_score included as an immediate antecedent. Regression was preferred over classification because both targets were continuous composite scores. These explanatory models are intended to estimate construct-level associations within the UTAUT framework; they are not used to demonstrate predictive superiority.

The BI equation is given by Equation (1), where β_0 is the intercept, β_1–β_6 are the regression coefficients, and ε is the error term. This equation estimates the association between each UTAUT construct and BI_score, controlling for the remaining constructs.

$$BI_{\text{score}} = \beta_0 + \beta_1 PE_{\text{score}} + \beta_2 EE_{\text{score}} + \beta_3 SI_{\text{score}} + \beta_4 FC_{\text{score}} + \beta_5 HM_{\text{score}} + \beta_6 HB_{\text{score}} + \varepsilon \tag{1}$$

The UB equation is given by Equation (2). This equation reflects the logic of the staged theory that BI should feed forward into enacted use, while direct construct effects may persist.

$$UB_{\text{score}} = \beta_0 + \beta_1 BI_{\text{score}} + \beta_2 PE_{\text{score}} + \beta_3 EE_{\text{score}} + \beta_4 SI_{\text{score}} + \beta_5 FC_{\text{score}} + \beta_6 HM_{\text{score}} + \beta_7 HB_{\text{score}} + \varepsilon \tag{2}$$

A structural equation model (SEM) was estimated as a model-level diagnostic using semopy, with the standardized path diagram. The model demonstrated excellent global fit, as indicated by χ^2 = 7.039 (p = 0.997), Comparative Fit Index (CFI) = 1.010, Tucker–Lewis Index (TLI) = 1.018, Goodness of Fit Index (GFI) = 0.994, Adjusted Goodness-of-Fit Index (AGFI) = 0.991, Normed Fit Index (NFI) = 0.994, and Root Mean Square Error of Approximation (RMSEA) = 0.000, alongside low information criteria (Akaike Information Criterion (AIC) = 31.933; Bayesian Information Criterion (BIC) = 85.487). Because some SEM software can return CFI and TLI values slightly above 1.00 under very strong model fit, these values were interpreted conventionally as approximately 1.00 rather than as evidence of "more than perfect" fit.

At the structural level, BI (BI_score) was most strongly associated with HM (β = 0.414, p < 0.001), followed by PE (β = 0.285, p < 0.001) and FC (β = 0.161, p = 0.008). In turn, UB (UB_score) was primarily driven by BI (β = 0.533, p < 0.001), with additional contributions from HB (β = 0.237, p < 0.001) and SI (β = 0.111, p = 0.029). Despite the excellent model fit, these estimates should be interpreted with caution due to substantial inter-construct correlations and severe multicollinearity. Accordingly, the SEM results are used as supportive structural evidence rather than definitive causal inference.

Figure 1 shows that the strongest paths into intention come from HM and PE, while the strongest path into behavior comes from BI itself. This supports the intended staged interpretation of the theory model. However, the diagram should still be read alongside the multicollinearity diagnostics rather than as a standalone confirmation of a fully validated structural model.

Figure 2 shows the correlation structure behind this caution. Several theoretically adjacent constructs were strongly correlated, particularly among PE, HM, BI, UB, FC, and HB. The figure shows that the strongest positive associations cluster among PE, HM, HB, BI, and UB. These associations are substantively plausible in a password security context, but they also foreshadow instability in coefficient-level interpretation if all constructs are modeled simultaneously. The multicollinearity diagnostics confirmed this concern.

While the correlation heatmap reflects only pairwise associations between variables, variance inflation factors (VIF) capture the extent to which each predictor can be explained by all other predictors simultaneously. As a result, VIF can be extremely high even when no single pairwise correlation appears excessively large.

In this study, multiple UTAUT constructs exhibited moderate-to-strong pairwise correlations, which collectively

Figure 1
Standardized SEM path diagram for the UTAUT model

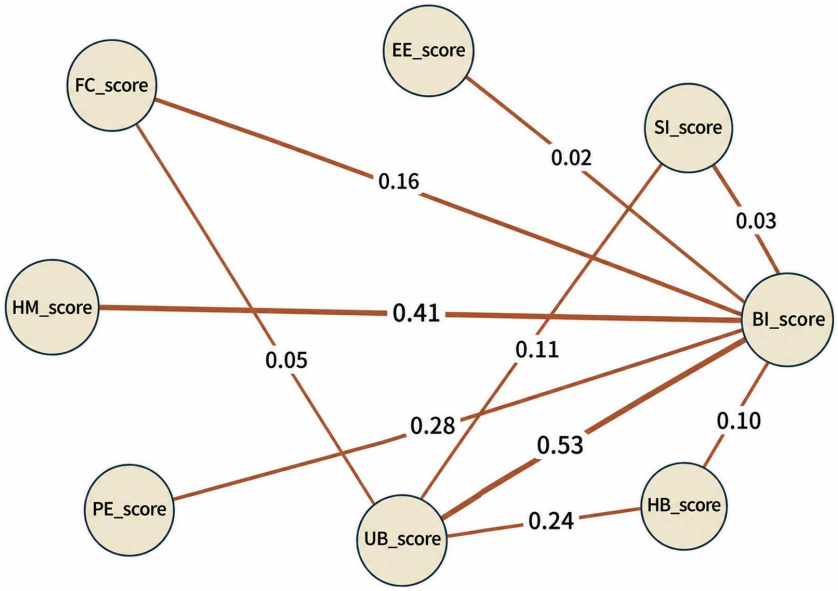
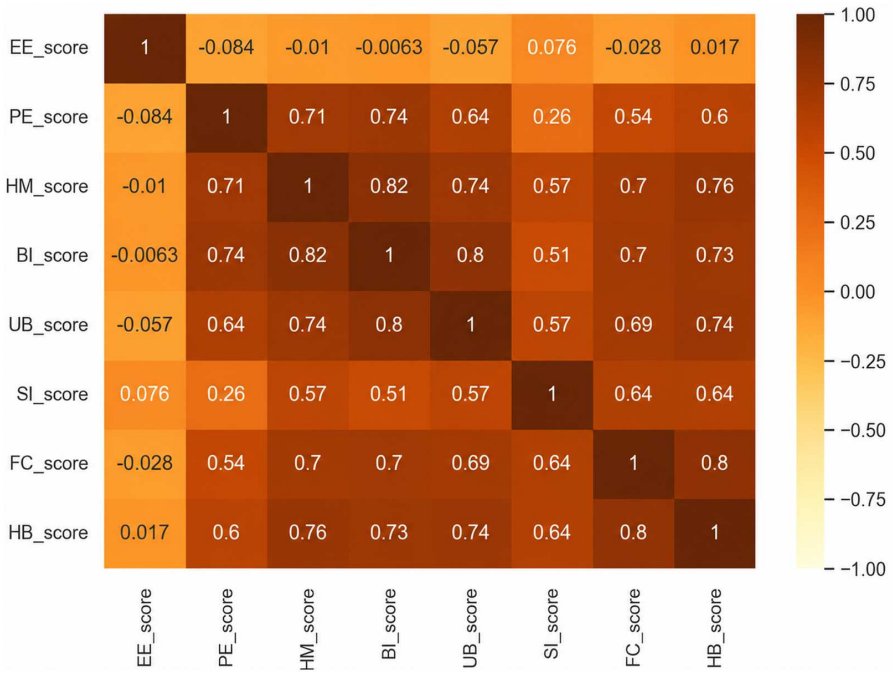


Figure 2
Correlation heatmap for the UTAUT-aligned composite scores



produced near-linear dependencies when modeled jointly. This multivariate redundancy explains the observed VIF values exceeding 100 and indicates that the predictors share substantial overlapping variance. Consequently, regression coefficients should be interpreted as conditional associations within a highly collinear system rather than as independent effects.

VIF values were modest for EE_score (3.10) but very high for the other core predictors, including PE_score (71.13), HM_score (119.07), SI_score (36.60), FC_score (88.16), and HB_score (128.88). VIF values exceeding 100 indicate severe redundancy among constructs, reinforcing that coefficient-level interpretations should be treated as conditional associations rather than independent effects. For that reason, coefficient signs and significance were interpreted as conditional associations within a highly overlapping system of constructs rather than as isolated causal effects. Such extreme VIF values indicate near-linear dependence among predictors, suggesting that the construct system behaves as a tightly coupled latent structure rather than a set of independent variables.

The highly correlated predictors were retained because they represent theoretically distinct UTAUT constructs rather than interchangeable statistical variables. Removing constructs solely based on VIF would weaken the model's theoretical interpretation and render the UTAUT structure incomplete. However, because VIF values were high for several predictors, the regression coefficients were interpreted as conditional associations within an overlapping construct system, rather than as independent causal effects. Ridge regression was then used in the predictive stage because regularization is more appropriate when predictors share substantial variance. This approach preserves the theory-driven construct structure while reducing the risk of overinterpreting unstable ordinary least-squares coefficients.

3.5. Predictive modeling

The sample size of 210 responses is acceptable for a focused, survey-based explanatory model. Still, it yields a relatively tight feature-to-sample ratio for machine learning, especially when both raw behavioral variables and integrated-feature sets are considered. For this reason, the predictive analysis emphasized cross-validation, parsimonious feature representations, and interpretable models rather than high-capacity algorithms. The results should therefore be interpreted as internally cross-validated predictive evidence within this institutional dataset, not as proof of generalizability to all educational institutions.

The predictive stage compared three feature-space strategies: construct-only, raw-features-only, and an integrated construct-plus-context feature set. Models included linear regression, ridge regression, random forest, support vector machine with Radial Basis Function (RBF) kernel, and gradient boosting. Five-fold cross-validation with a fixed seed was used throughout. Predictive model comparison answers a different question than explanatory regressions: which feature representation generalizes best out-of-sample [6, 7].

The generic machine learning prediction equation can be written as Equation (3), where X denotes the selected predictor matrix and $f(\cdot)$ represents the fitted model. In this study, $\hat{y}$ corresponds to a continuous prediction of BI_score or UB_score.

$$\hat{y} = f(X) \tag{3}$$

Because the primary outcomes are continuous composite scores, model performance was evaluated using RMSE, MAE, and cross-validated R^2. To satisfy classification-based reporting without replacing the continuous design, a secondary sensitivity analysis was conducted by converting the targets into high-endorsement binary outcomes using a fixed cutoff (score $\geq$ 6.0). For this supplementary analysis, the classification loss is defined as in Equation (4).

$$L = -\Sigma_i \left[y_i \, log(\hat{y}_i) + (1 - y_i) \, log(1 - \hat{y}_i) \right] \tag{4}$$

This cross-entropy formulation penalizes confident incorrect classifications. In this study, classification metrics are reported

only as supporting evidence because dichotomizing BI_score and UB_score reduces information compared with their continuous forms.

Deep learning models were not pursued as a design choice in this study. The dataset is relatively small, the variables are tabular and survey-based, and the study prioritizes interpretable and statistically defensible comparisons over increased model complexity. This reflects a methodological choice rather than a limitation.

3.6. Association rule mining

ARM was applied because the dataset includes binary and discretizable password-behavior indicators, as well as categorized construct-score states (e.g., high vs low levels). Transactional data were therefore constructed from interpretable conditions such as password_reuse, recover_capable, random_attackable, strong_composition, and high-score construct markers. Extracted rules were evaluated using standard metrics, including support, confidence, lift, leverage, and conviction, and subsequently filtered to remove redundant or trivial patterns [18, 25].

The core ARM metrics are defined in Equations (5)–(7). Support measures the proportion of observations in which the antecedent (A) and consequent (B) occur together.

$$support(A \rightarrow B) = P(A \cap B) \tag{5}$$

Confidence measures the conditional probability that the consequent occurs given that the antecedent is present.

$$confidence(A \rightarrow B) = P(B \mid A) \tag{6}$$

Lift compares the observed co-occurrence of A and B to the expected co-occurrence under statistical independence. Values greater than 1.0 indicate a positive, nonrandom association between the antecedent and consequent.

$$lift(A \rightarrow B) = P(A \cap B) / [P(A)\,P(B)] \tag{7}$$

In this study, the ARM stage is treated as descriptive pattern discovery rather than formal hypothesis testing. To provide a baseline for interpretation, a lightweight null comparison based on column-wise permutation was employed to assess whether observed lift values exceed chance-level co-occurrence. While this approach adds analytical rigor, it does not establish causal, temporal, or directional relationships [18, 25].

4. Results

4.1. Descriptive and measurement results

The dataset shows that respondents generally have favorable attitudes toward password-protective behavior. Mean scores were high for PE, HM, BI, UB, FC, and HB, while EE items were much lower in absolute mean terms. Practically, this suggests that respondents reported password-protective behavior as useful and routine, but not necessarily effortless. This pattern is consistent with cybersecurity behavior research showing that users may recognize the value of protective practices while still experiencing usability, memory, and routine-formation barriers in everyday password management [1–5].

The reliability results reported in Table 1 support the continued use of the composite variables in the remaining analyses. At the same time, the strong construct correlations shown in Figure 2 suggest that respondents may not sharply distinguish among several favorable orientations toward password management. That overlap matters for interpreting the regression coefficients below because closely related favorable orientations can become difficult to separate in simultaneous models, particularly when technology-acceptance constructs are theoretically interrelated [19, 20, 23, 24].

4.2. Explanatory UTAUT findings

Table 2 reports the construct-level regression estimates for the two explanatory models. The standardized beta column is treated as the comparable effect-size indicator across predictors. For BI_score, the model explained 75.3% of the variance (R^2 = 0.753, adjusted R^2 = 0.746, F = 103.360, p < 0.001; RMSE = 0.475).

Table 2
Explanatory regression results for behavioral intention and use behavior

Target	Predictor	*b*	β	*p*	95% CI
BI	HM	0.395	0.414	<0.001	[0.273, 0.518]
BI	PE	0.258	0.285	<0.001	[0.162, 0.353]
BI	FC	0.141	0.162	0.010	[0.034, 0.248]
BI	EE	0.013	0.023	0.524	[–0.027, 0.054]
BI	SI	0.019	0.026	0.615	[–0.054, 0.091]
BI	HB	0.102	0.104	0.125	[–0.029, 0.233]
UB	BI	0.462	0.444	<0.001	[0.306, 0.618]
UB	HB	0.210	0.206	0.006	[0.062, 0.359]
UB	SI	0.108	0.142	0.010	[0.026, 0.190]
UB	EE	–0.036	–0.059	0.124	[–0.081, 0.010]
UB	PE	0.096	0.102	0.101	[–0.019, 0.211]
UB	HM	0.039	0.039	0.612	[–0.112, 0.190]
UB	FC	0.033	0.037	0.592	[–0.089, 0.155]

Note: *b* = unstandardized coefficient; β = standardized coefficient; CI = confidence interval. BI = behavioral intention; UB = use behavior; HM = hedonic motivation; PE = performance expectancy; FC = facilitating conditions; EE = effort expectancy; SI = social influence; HB = habit.

HM was the strongest predictor (β = 0.414, b = 0.395, p < 0.001, 95% CI [0.273, 0.518]), followed by PE (β = 0.285, b = 0.258, p < 0.001, 95% CI [0.162, 0.353]) and FC (β = 0.162, b = 0.141, p = 0.010, 95% CI [0.034, 0.248]). These results suggest that stronger BI is primarily associated with perceived value, experiential engagement, and supportive conditions. This pattern is consistent with UTAUT and UTAUT2 perspectives, which emphasize PE, FC, HM, and HB in technology-related behavior [16–21].

For UB_score, the model explained 71.2% of the variance (R^2 = 0.712, adjusted R^2 = 0.702, F = 71.449, p < 0.001; RMSE = 0.534). BI was the dominant predictor (β = 0.444, b = 0.462, p < 0.001, 95% CI [0.306, 0.618]), followed by HB (β = 0.206, b = 0.210, p = 0.006, 95% CI [0.062, 0.359]) and SI (β = 0.142, b = 0.108, p = 0.010, 95% CI [0.026, 0.190]). This pattern is theoretically consistent and indicates that UB is associated with BI, reinforced by habit formation, and shaped by social context. These results support a staged behavioral process in which intention mediates the effects of core constructs, while HB and SI sustain actual behavior over time, consistent with the logic of UTAUT/UTAUT2 and prior cybersecurity behavior studies emphasizing routines, responsibility, and social-organizational context [9–11, 15–17].

The differences between SEM in Figure 1 and regression estimates in Table 2 arise from their distinct modeling assumptions. Regression coefficients represent partial effects under strict multicollinearity control, whereas SEM estimates are derived from a system-level covariance structure that explicitly models shared variance among constructs. Given the high inter-construct correlations observed in this dataset, regression results provide more conservative estimates of independent effects, while SEM reflects broader structural associations. As such, the two approaches are complementary rather than contradictory, with SEM used for structural validation and regression used for more stable inferential interpretation [6, 8, 16, 17, 23].

Figure 3 visualizes the relative standardized effects across the explanatory models, reinforcing the separation between the two dependent variables. BI is led by HM and PE, whereas UB is led by intention itself and HB. The visual pattern supports a staged theoretical interpretation within a UTAUT framework rather than a single, undifferentiated claim about "technology acceptance" [16, 17, 20, 23, 24].

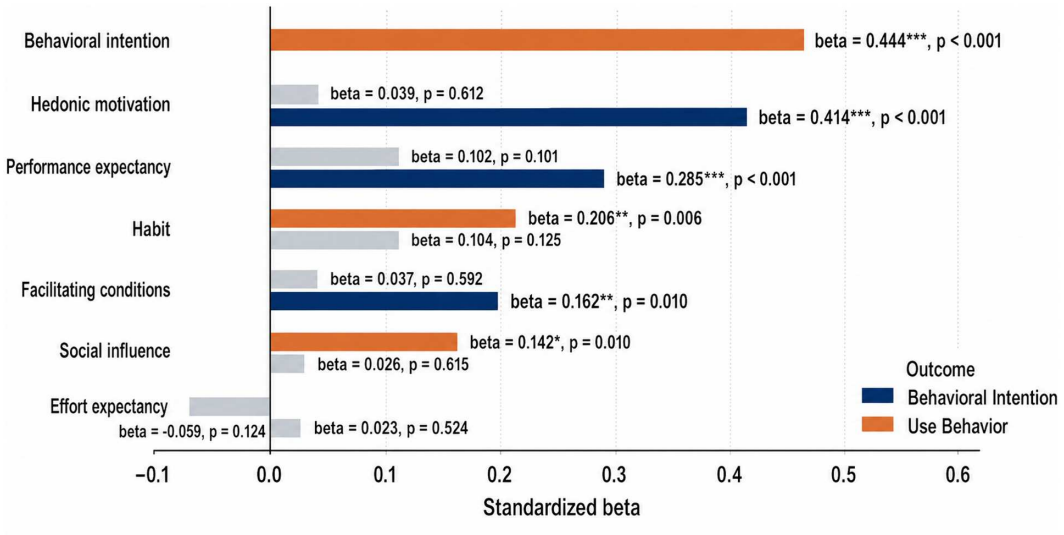
4.3. Predictive machine learning results

The comparative pattern observed here is consistent with recent cybersecurity behavior and password security studies using structured survey data, which report that classical and ensemble machine learning models often yield modest and statistically comparable performance when evaluation is rigorously controlled and data dimensionality is limited. Recent cybersecurity machine learning reviews emphasize that random forest, support vector machine, regularized linear models, and gradient boosting remain competitive in behavioral and organizational security settings, and that performance gains from increasing model complexity are typically incremental rather than decisive when sample sizes are moderate. In the present study, the feature spaces were theory-driven [6, 7, 26, 27]. In this context, the present results reinforce a growing consensus that feature representation, construct validity, interpretability, and evaluation discipline matter more than algorithm selection alone in applied cybersecurity behavior modeling [7, 8, 26, 27].

Table 3 summarizes the best-performing predictive models across feature families. The key finding from this table is that construct-only ridge regression achieved the best overall predictive performance for both outcomes. For BI_score, the model obtained RMSE = 0.491, MAE = 0.373, and mean R^2 = 0.650, outperforming the best integrated and raw-feature models by 0.014 and 0.007 RMSE, respectively. For UB_score, the construct-only model achieved RMSE = 0.553, MAE = 0.391, and mean R^2 = 0.640, with performance gains of 0.023 RMSE over raw features and 0.053 RMSE over integrated models.

However, fold-level paired comparisons indicate that ridge regression did not significantly outperform standard linear regression. For BI_score, the mean fold Mean Squared Error (MSE) difference was −0.00014 (95% CI [−0.00063, 0.00034], paired t p = 0.460; Wilcoxon p = 0.438; d = −0.365). For UB_score, the difference was −0.00053 (95% CI [−0.00243, 0.00136], paired t p = 0.479; Wilcoxon p = 0.438; d = −0.349). These results support a conclusion of parsimony rather than

Figure 3
Standardized theory effects for the construct-level explanatory models



Colored bars indicate p < 0.05; grey bars are not statistically significant.
Asterisks denote significance levels (* p < 0.05, ** p < 0.01, *** p < 0.001).

Table 3
Best cross-validated predictive models by target and feature family

Target	Features	Model	RMSE	MAE
BI_score	Construct-only	Ridge regression	0.491	0.373
BI_score	Raw features	Best model	0.498	–
BI_score	Integrated features	Best model	0.505	–
UB_score	Construct-only	Ridge regression	0.553	0.391
UB_score	Raw features	Best model	0.576	–
UB_score	Integrated features	Best model	0.606	–

Note: Lower RMSE and MAE indicate better predictive performance. The construct-only ridge model achieved the lowest RMSE for both BI_score and UB_score, supporting the conclusion that aggregated UTAUT constructs provided the most stable out-of-sample signal. Missing MAE values for non-leading feature families indicate that only the main comparative RMSE values were retained for those configurations.

clear algorithmic superiority: simpler, theory-based representations perform as well as more complex alternatives. Importantly, these findings reflect only predictive performance and do not imply that stronger out-of-sample accuracy corresponds to greater theoretical importance, consistent with the distinction among explanation, prediction, and practical significance [6–8].

The finding that construct-only ridge regression performed best does not imply that all raw password-behavior indicators are irrelevant. Rather, it indicates that, in this sample, the aggregated constructs captured the strongest generalizable signal for BI_score and UB_score. Raw and integrated-feature spaces may have contained useful information, but they also increased dimensionality and redundancy relative to the sample size. This explains why expanded feature sets did not improve out-of-sample performance and supports the methodological value of parsimonious, interpretable, theory-grounded feature construction [8, 16, 17, 26, 27].

Figure 4 shows that broader feature inclusion did not improve prediction in this sample. Instead, the more parsimonious construct-only representation generalized slightly better. This represents a theoretically and methodologically important negative finding: adding contextual and behavioral variables increased dimensionality without producing a consistent out-of-sample gain. This result is consistent with the view that predictive modeling should be evaluated empirically rather than assuming that larger feature spaces or more flexible algorithms automatically improve performance [6–8, 26, 27].

Figure 5 provides an ablation-style overview of error shifts across feature-set comparisons. The figure shows that removing or simplifying some feature groups did not yield substantial changes in performance, consistent with the high shared variance among constructs and the strong performance of aggregated theory-based features. The limited differences should not be interpreted as evidence that the removed constructs are unimportant. Instead, they indicate that several constructs contain overlapping predictive information in this dataset. This finding supports the use of parsimonious construct-level modeling and reinforces the need for cautious interpretation of individual coefficients in the presence of multicollinearity [16, 17, 20, 23].

Several ablation conditions produced identical or near-identical performance because the removed predictors shared substantial variance with retained constructs. In highly correlated survey data, deleting one construct may not substantially reduce predictive performance if other constructs carry similar information. Therefore, the identical or near-identical ablation results should be interpreted as evidence of redundancy and robustness, not as evidence that the constructs are theoretically meaningless. This pattern also helps explain why ridge regression performed well: regularization can stabilize prediction when theoretically related variables overlap [20, 26, 27].

Explainability analysis is also aligned with the explanatory models. For BI_score, permutation importance ranked HM_score highest (importance mean = 0.336, SD = 0.031), followed by PE_score (0.168, SD = 0.017) and FC_score (0.052, SD = 0.010). For UB_score, the dominant predictor was BI_score (0.370, SD = 0.031), followed by HB_score (0.076, SD = 0.014) and SI_score (0.035, SD = 0.009). Figure 6 visualizes these rankings and shows convergence between the explanatory and predictive results. The features that mattered most for prediction were largely the same constructs that mattered in the explanatory regressions. That convergence strengthens confidence in the substantive interpretation, even though explanation and prediction remain distinct tasks [6–8].

4.4. Supplementary classification sensitivity results

Table 4 reports the secondary classification sensitivity analysis requested for accuracy, precision, recall, F1, and Receiver Operating Characteristic-Area Under the Curve (ROC-AUC). The analysis used fixed high-endorsement cutoffs rather than data-mined thresholds: BI_high_6plus was coded as 1 when BI_score was greater than or equal to 6.0, and UB_high_6plus was coded as 1 when UB_score was greater than or equal to 6.0. This yielded 127 high cases versus 83 lower cases for BI_score, and 106 high cases versus 104 lower cases for UB_score. The table also shows that classification performance was moderate rather than exceptional, reinforcing the need to treat the binary results as sensitivity evidence rather than as the main analytical design [6–8].

For BI_high_6plus, the raw-feature random forest achieved an ROC-AUC of 0.770 and a high recall of 0.890, indicating it identified most high-intention respondents but did not fully displace the primary continuous regression result. For UB_high_6plus, construct-only gradient boosting produced ROC-AUC = 0.789, F1 = 0.753, and accuracy = 0.729, again supporting the conclusion that theory-grounded construct information remains highly predictive. These metrics provide supplementary evidence of robustness. However, they should not be interpreted as superior to continuous-outcome models, as dichotomization reduces information and alters the interpretation of the outcome [6, 8].

Figure 4
Comparative predictive performance of the strongest models across feature-family strategies

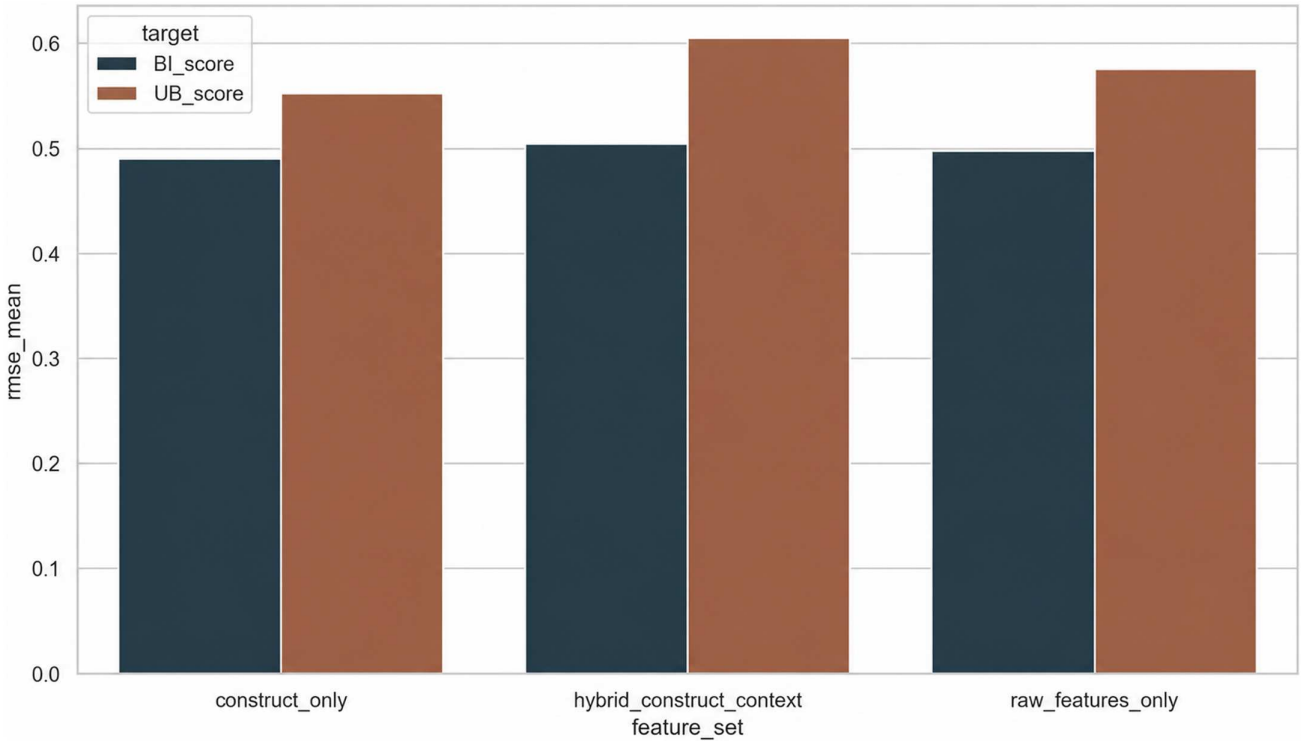


Figure 5
Ablation overview representing error shifts across key feature-set comparisons

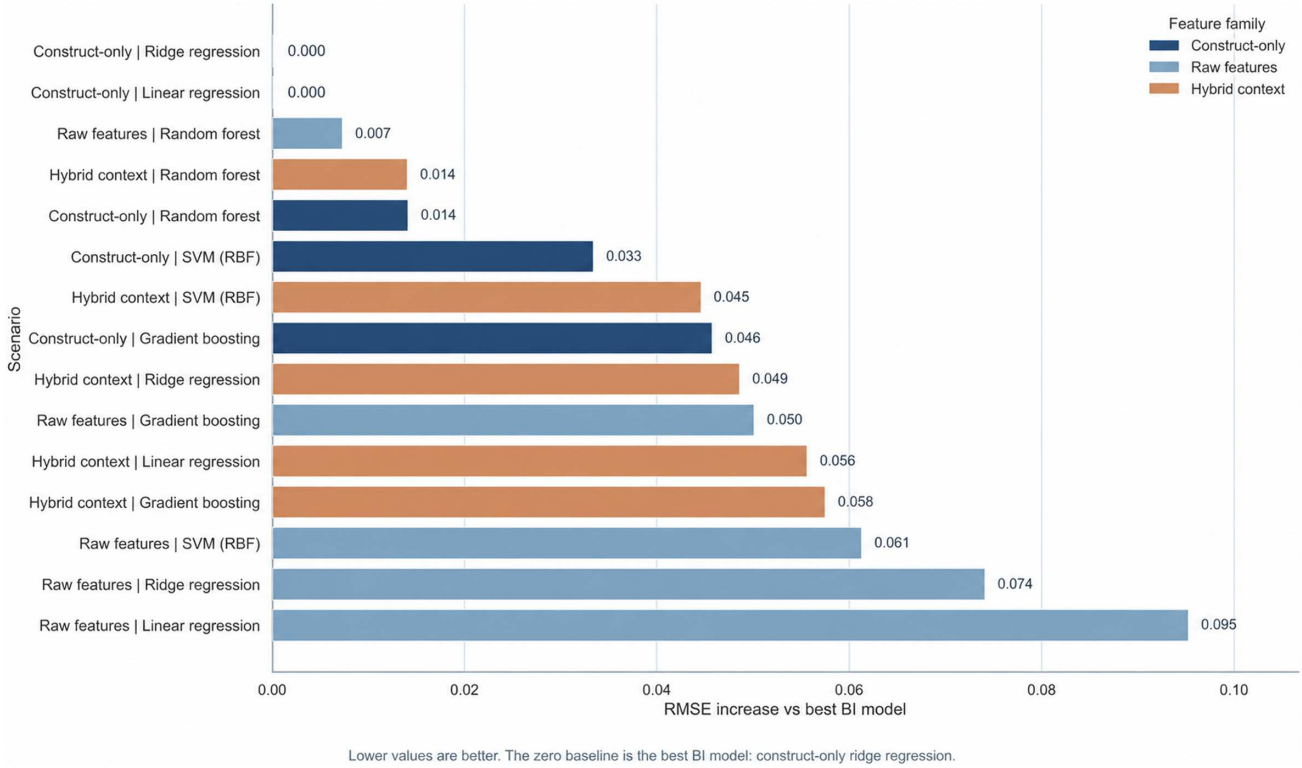


Figure 6
Permutation feature importance for the best-performing construct-only ridge models

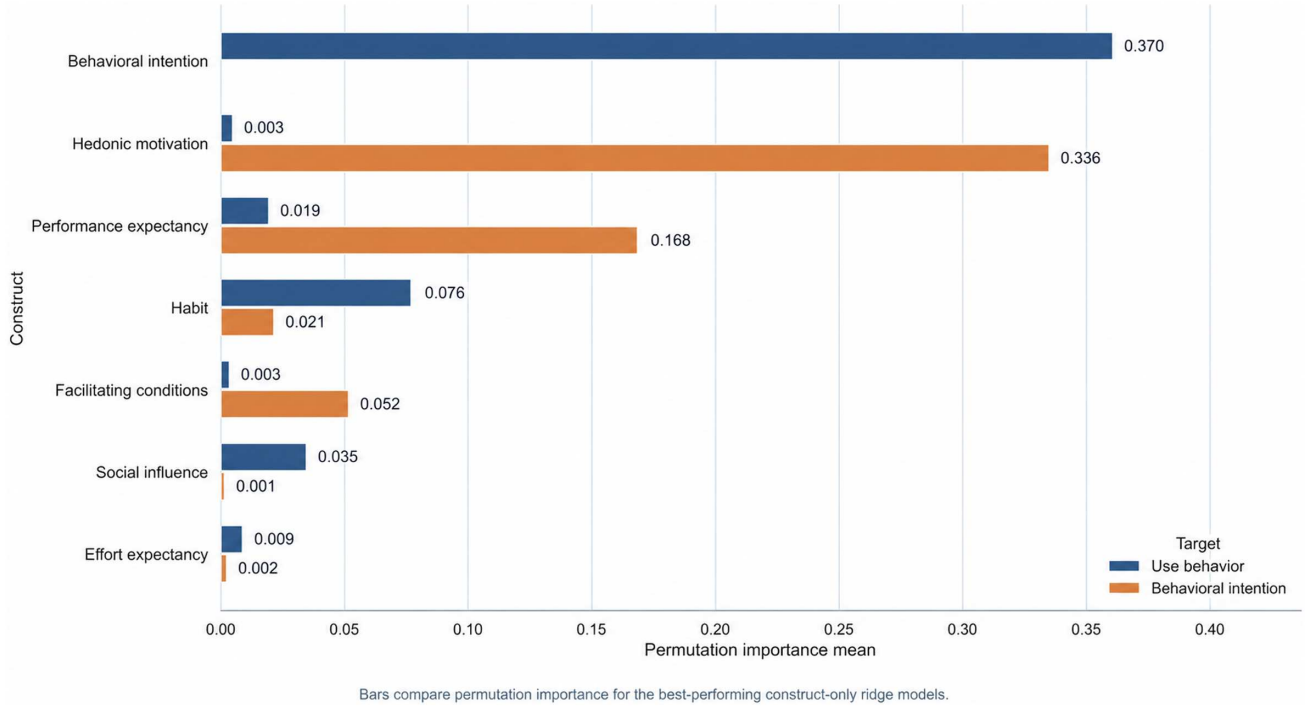


Table 4
Best supplementary classification models for high-endorsement outcomes

Target	Model	Feat	Acc	Prec	Rec	F1	AUC
BI≥6	RF	Raw	0.719	0.716	0.890	0.792	0.770
UB≥6	GB	Const	0.729	0.703	0.812	0.753	0.789

Note: BI≥6 = BI_score ≥ 6.0; UB≥6 = UB_score ≥ 6.0. RF = random forest; GB = gradient boosting; Feat = feature set; Raw = raw behavioral features; Const = construct-level features. Acc = accuracy; Prec = precision; Rec = recall; AUC = area under the ROC curve.

4.5. Association rule mining results

Table 5 presents the strongest association rules identified from the dataset, highlighting consistent co-occurrence patterns centered on high SI (high_SI) as the dominant consequent. Across all rules, confidence values are high (0.869–0.917), indicating that when the antecedent conditions are present, the likelihood of observing strong SI is substantial. These rules are interpreted as descriptive co-occurrence patterns rather than causal or temporal relationships, in line with ARM guidance that supports the view that confidence and lift describe pattern strength rather than causal direction [18, 25].

The most prominent rule, combining high FC with recovery capability, achieves the highest confidence (0.917) and lift (1.689), suggesting a strong, nonrandom association. Similarly, rules involving recovery capability combined with HB, HM, or UB also yield elevated lift values (1.601–1.641), reinforcing the central role of user support and behavioral readiness. Such results are useful for institutional interpretation because they identify co-occurring support and behavior states, but they should remain descriptive rather than causal [18, 25].

Leverage values (0.051–0.107) and conviction scores (3.486–5.486) further confirm that these patterns are not due to chance and exhibit meaningful dependence. Notably, the repeated presence of recovery capability across multiple rules indicates that the ability to manage and recover passwords is a key behavioral anchor linked to stronger SI.

The results suggest that FC, recovery competence, and habitual engagement co-occur with socially reinforced security

Table 5
Selected high-value association rules

Antecedent → Consequent	Supp	Conf	Lift
high_FC + recover_capable → high_SI	0.262	0.917	1.689
high_UB + password_reuse → high_SI	0.129	0.900	1.658
recover_capable + high_HB → high_SI	0.271	0.891	1.641
high_UB + recover_capable → high_SI	0.229	0.889	1.637
recover_capable + high_HM → high_SI	0.252	0.869	1.601

Note: Supp = support; Conf = confidence. Rules are interpreted as descriptive co-occurrence patterns, not as causal, temporal, or directional relationships. A lift value greater than 1.0 indicates that the antecedent and consequent co-occur more often than expected under independence.

behavior, providing actionable insight into how support structures and routines interact within password security practices. These findings reinforce the view that effective password security behavior emerges from the interaction of support, capability, routine, and social reinforcement rather than isolated individual factors [9–13].

Figure 7 summarizes the support-confidence-lift structure of the retained rules, showing the rule set is not driven only by rare, unstable patterns. Several retained rules combine moderate support with meaningfully elevated lift, making them more useful for interpretation than extreme but sparsely supported rules [18, 25].

Figure 8 reveals repeated concentration around high_SI_score, recover_capable, high_HB_score, high_FC_score, and related high-score states. This matters because it complements the regression results: SI and HB were not only isolated coefficient-level findings but also part of a broader co-occurrence structure.

Figure 7
Support, confidence, and lift distribution of retained association rules

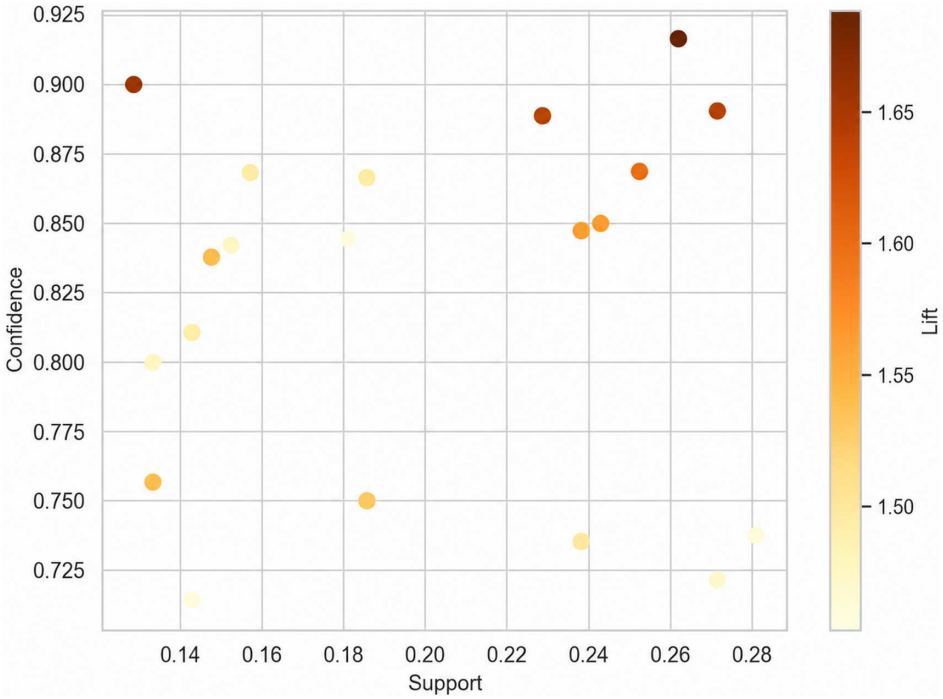
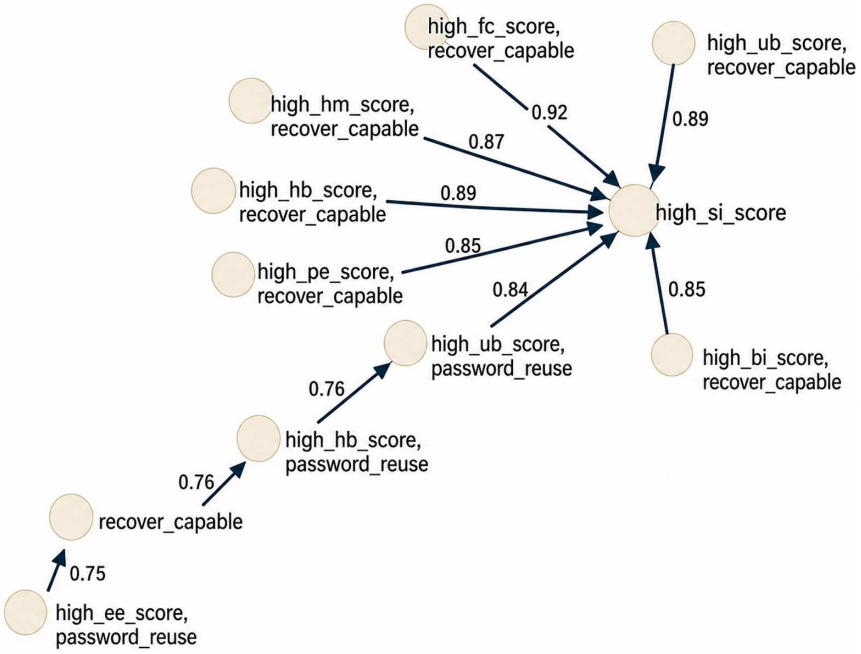


Figure 8
Network representation of the strongest retained association rules



This supports an integrated interpretation in which password behavior is shaped by both acceptance constructs and practical support conditions [15–17].

Figure 9 represents the most frequently retained itemsets. The itemset profile indicates that several theoretically meaningful states were common enough to support ARM interpretation, including high BI_score (support = 0.605), high UB_score (0.505), high HB_score (0.586), high FC_score (0.571), high SI_score (0.543), and recover_capable (0.490). This helps justify why ARM was methodologically feasible in this dataset.

Figure 10 presents the ranking of the top rules by lift, showing that the retained rules had lift values above the permutation-based reference level. The average observed lift among retained rules was 1.537 versus a null-style permutation baseline of 1.001, leaving an observed-minus-null gap of 0.536. Even so, these are still descriptive co-occurrence patterns and should not be interpreted as directional, temporal, or causal effects [18, 25].

5. Discussion

5.1. Integrated interpretation of explanatory, predictive, and ARM findings

The findings show that a combination of motivation, perceived value, support, habit, and social context shapes password security behavior among educational personnel. In the explanatory models, BI was most strongly associated with HM, PE, and FC. This indicates that respondents reported stronger intentions to follow secure password practices when they perceived those practices as useful, well supported, and not excessively burdensome. UB followed a staged pattern: BI was the strongest correlate of UB, while HB and SI provided additional explanatory value. This suggests that password security behavior is not only a matter of individual attitude but also a repeated workplace routine shaped by institutional norms and peer influence, consistent with UTAUT/UTAUT2 and recent research on cybersecurity behavior [9–11, 15–17].

The predictive results complement this interpretation. Construct-only ridge regression achieved the best cross-validated performance for both BI_score and UB_score, although its advantage over standard linear regression was not statistically significant. This supports a conclusion of parsimony rather than algorithmic superiority. In this dataset, aggregated UTAUT constructs captured the strongest generalizable signal, while raw behavioral features and integrated-feature spaces added dimensionality without improving out-of-sample performance. The supplementary classification analysis further supports this conclusion: classification metrics were useful as sensitivity evidence, but continuous-outcome prediction remained the primary and more information-preserving analytical design [6–8, 26, 27].

The ARM results add a descriptive co-occurrence perspective. The strongest rules repeatedly involved recovery capability, FC, HB, SI, and high scores for BI or UB. These patterns suggest that secure password behavior is embedded in bundles of enabling and normative conditions rather than isolated single-variable tendencies. Importantly, the rules should not be interpreted as causal or temporal mechanisms. They show that certain behavioral and perceptual states tend to co-occur, not that one condition causes another [18, 25]. The presence of password reuse in some high-lift rules is especially important because it shows that favorable self-reported security orientations may coexist with imperfect operational practices, a concern consistent with prior studies of password security and cybersecurity behavior [2, 5, 12–15].

Figure 9
The most common retained item sets used for ARM interpretation

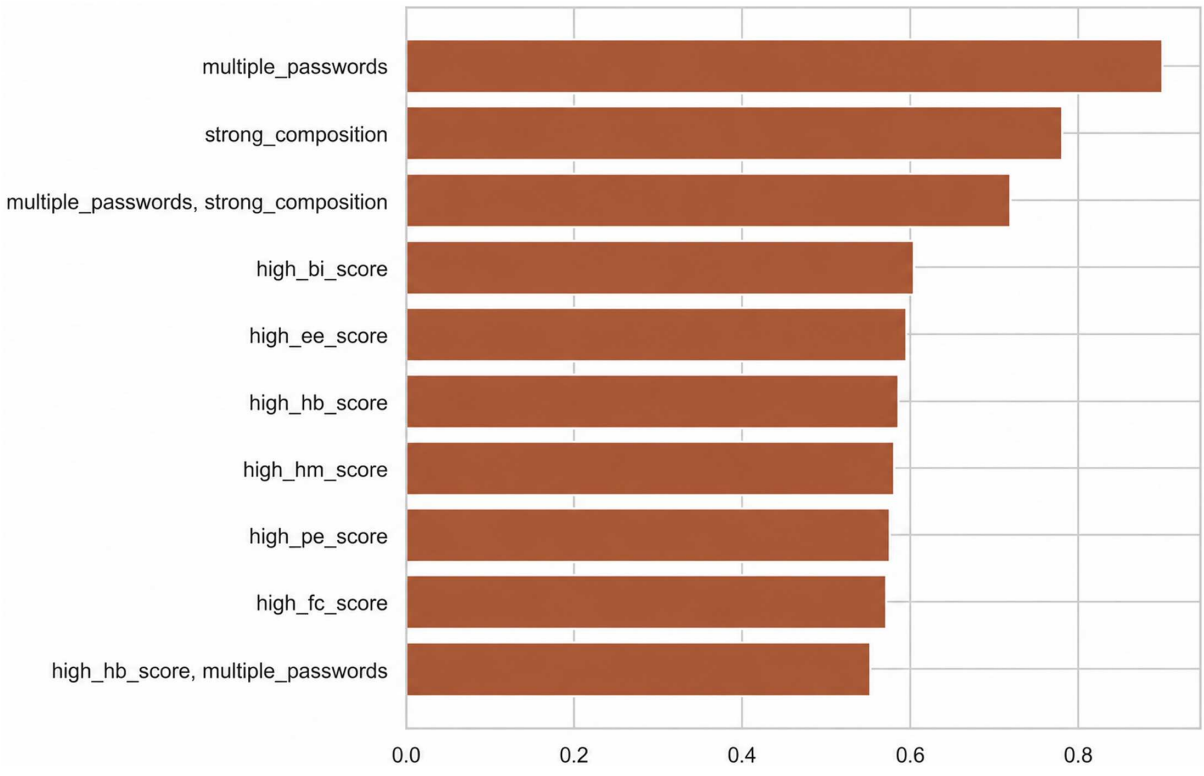
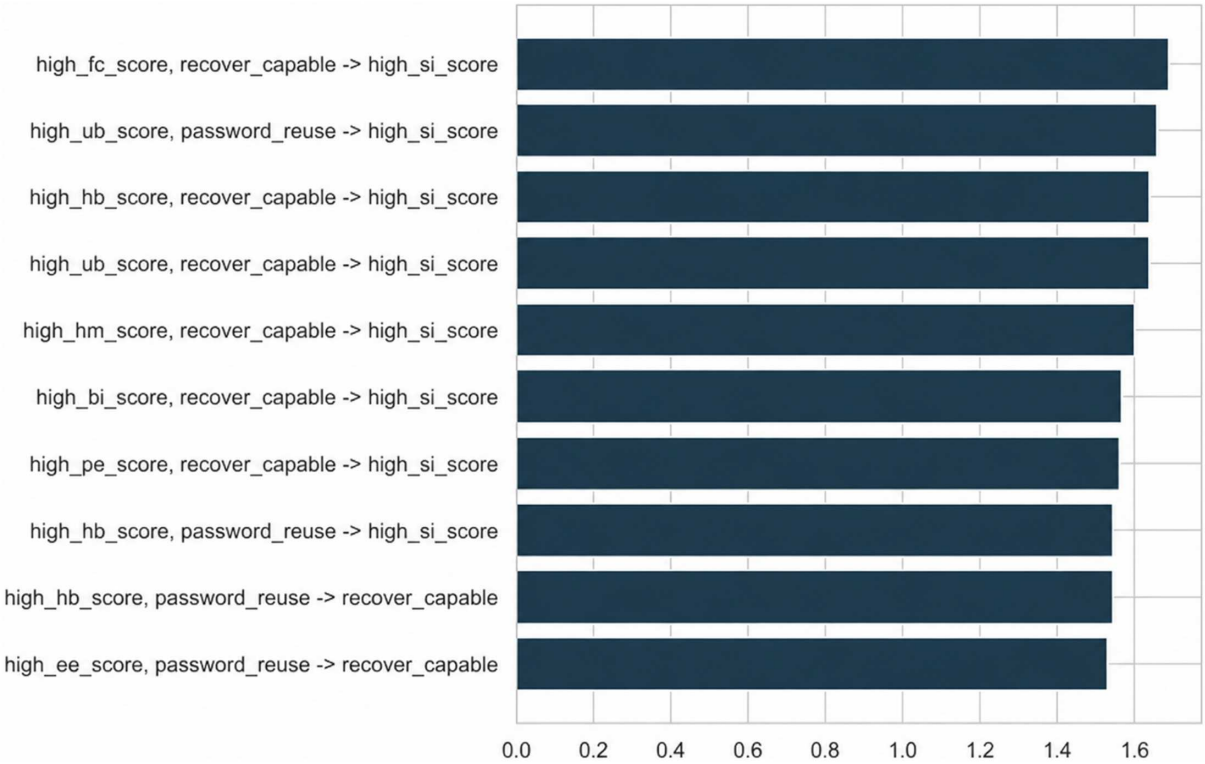


Figure 10
Top retained association rules ranked by lift



Across the three analytical streams, there is more convergence than contradiction. Regression identifies the strongest conditional associations, machine learning evaluates out-of-sample prediction, and ARM reveals co-occurring behavioral states. Together, these results show that theoretically structured constructs can provide both explanatory clarity and competitive predictive performance, while also revealing practical tensions between self-reported orientation and actual password-management routines [6–8]. The severe multicollinearity among UTAUT constructs does not invalidate the study, but it does shape interpretation. Because users who perceive password security as useful may also perceive it as habitual, supported, and socially reinforced, high construct overlap is substantively plausible. The appropriate response is therefore to avoid overclaiming individual coefficients and to interpret the construct system as an overlapping behavioral environment [16, 17, 20, 23, 24].

5.2. Theoretical, methodological, and empirical contributions

This study contributes to cybersecurity behavior research in four ways. First, it provides a theoretical contribution by showing that a UTAUT-based framework remains useful for explaining password security behavior in an educational setting. HM, PE, FC, BI, HB, and SI emerged as important signals across the explanatory and predictive stages, aligning with UTAUT/UTAUT2 and higher-education technology-adoption literature [16–20]. Second, it contributes methodologically by clearly separating explanation, prediction, and ARM. This distinction is important because statistical significance, predictive accuracy, and co-occurrence patterns represent different types of evidence and should not be interpreted as interchangeable [6–8, 18, 25].

Third, the study makes an empirical contribution by showing that construct-only models can outperform broader raw-feature and integrated-feature spaces in cross-validation. This challenges the assumption that adding more variables or using more complex feature spaces necessarily improves predictive performance. In structured survey datasets with modest sample sizes and highly related constructs, theoretically grounded aggregation may provide a more stable representation than expanded feature spaces [6–8, 26, 27]. Fourth, the study contributes practically by identifying actionable intervention domains, including recovery capability, FC, habit formation, and socially reinforced security routines, which are consistent with prior work on cybersecurity behavior change, password-manager adoption, and protective behavior support [13–15].

5.3. Practical implications for educational cybersecurity policy

The findings provide practical guidance for Krabi Technical College and similar educational institutions. First, institutions should strengthen password-support infrastructure. Clear password-recovery procedures, accessible help desk support, step-by-step reset guidance, and regular communication about where to obtain assistance can improve users' confidence in managing password problems. The association rules involving recovery capability and FC suggest that support infrastructure is not merely a technical service but part of the behavioral environment that sustains secure practice. This implication is consistent with studies of cybersecurity behavior that emphasize usability, coping support, password-management capability, and institutional facilitation [9–12].

Second, cybersecurity training should be routine based rather than limited to occasional awareness sessions. Because

HB was important for UB and appeared repeatedly in the co-occurrence structure, institutions should introduce periodic password health checks, recurring micro-training, password-manager demonstrations, and scheduled reminders. These activities can help transform secure password practices from an abstract policy requirement into a routine workplace practice, consistent with behavior-change and cybersecurity-intervention perspectives [10–13].

Third, password security should be framed as a shared institutional responsibility. SI appeared in the explanatory model and as the dominant consequent in several association rules. Departments can therefore support password security by appointing digital-safety champions, encouraging peer reminders, involving supervisors in communication campaigns, and normalizing secure password practices as part of everyday professional responsibility. This implication aligns with research showing that cybersecurity behavior is shaped by social, organizational, and responsibility-based factors, not only by individual knowledge [9–11, 15].

Fourth, password reuse remains a policy concern even among respondents with favorable security orientations. Institutions should combine training with technical safeguards, including password-manager support, multi-factor authentication, password reuse warnings, and clear guidance discouraging the reuse of the same password across institutional and personal systems. These actions translate the integrated UTAUT, machine learning, and ARM findings into practical cybersecurity administration and align with prior studies on password behavior, password-manager adoption, and cybersecurity behavior change [2, 5, 12–14].

5.4. Limitations and future research

Several limitations should guide interpretation. The study used 210 survey responses from a single educational institution, which limits generalizability and constrains subgroup analysis. The construct system showed severe multicollinearity, so coefficient-level interpretations should be treated as conditional associations rather than independent causal effects. The data were self-reported and cross-sectional, which limits causal inference and may increase common method overlap [28]. The ARM component depended on discretization choices and used supportive rather than exhaustive validation [18, 25]. In addition, the supplementary classification analysis used a fixed high-endorsement threshold, so accuracy, precision, recall, F1, and ROC-AUC should be treated as secondary sensitivity metrics rather than as the primary evaluation standard [6, 8].

The sample size-to-feature ratio should also be considered when interpreting machine learning results. Although construct aggregation, ridge regression, and five-fold cross-validation reduce the risk of overfitting, more complex models require larger and more diverse datasets before their performance can be assessed reliably. The findings are therefore best interpreted as evidence from one institutional context, not as a general benchmark for all educational personnel. This caution is consistent with the broader machine learning and cybersecurity analytics literature, which emphasizes validation discipline, interpretability, and external testing before deployment [6, 7, 26, 27].

Future research should test the framework using larger samples, multiple educational institutions, longitudinal designs, and, where available, objective system-use indicators. Larger datasets would enable more stable comparisons of nonlinear machine learning models and better subgroup analyses by role, age, digital literacy, and institutional unit. Longitudinal or intervention-based studies could examine whether changes in training, password policy, recovery support, or technical safeguards lead to measurable improvements in password behavior. Future studies should also compare self-reported UTAUT constructs with objective cybersecurity logs to determine how closely perceived security orientation aligns with actual password-management practices [5, 15, 28, 29].

6. Conclusion

This study examined password security behavior among educational personnel at Krabi Technical College using an integrated framework that combines UTAUT, machine learning, and ARM. The study showed that BI was most strongly associated with HM, PE, and FC. At the same time, UB was most strongly associated with BI, HB, and SI. These findings support the continued relevance of UTAUT/UTAUT2 for explaining security-related technology behavior in educational and organizational settings [16, 17, 19, 20]. Construct-only ridge regression provided the best cross-validated predictive performance for both BI_score and UB_score, although its advantage over standard linear regression was not statistically significant. ARM added complementary descriptive insight by identifying co-occurrence patterns involving recovery capability, FC, HB, and SI. Overall, the study demonstrated that theory-driven construct representations can provide both explanatory clarity and competitive predictive performance when measuring password security behavior using survey data [18, 25–27].

Future work should validate the framework using larger, more diverse institutional samples, longitudinal behavioral data, and, where available, actual system-use indicators. Educational institutions should translate the findings into practical cybersecurity actions, including clearer password-recovery support, routine password-management training, peer-supported security norms, password-manager guidance, and technical safeguards against password reuse. Future studies should also compare the predictive value of UTAUT constructs with objective cybersecurity logs and evaluate whether targeted interventions improve actual password behavior over time, especially given prior evidence that cybersecurity behavior depends on knowledge, usability, responsibility, habit, coping support, and practical password-management capability [9–13].

Ethical Statement

All subjects provided informed consent for inclusion before participating in the study. The study was conducted in accordance with the Declaration of Helsinki, and the protocol was approved by the Human Research Ethics Committee of the Phuket Rajabhat University, Thailand (Reference No.: PKRU2567/07).

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The data that support the findings of this study are openly available in GitHub at https://github.com/pjarupunphol/Datasets/blob/main/Krabi_Technical.zip.

Author Contribution Statement

Pita Jarupunphol: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration. **Sujira Jeennoo:** Conceptualization, Validation, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Project administration.

References

[1] Barakovic, S., & Barakovic Husic, J. (2023). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective*, *32*(5), 347–370. https://doi.org/10.1080/19393555.2022.2088428

[2] Titiakarawongse, C., & Boonkrong, S. (2023). A study of password management behaviors of young people. *Applied Science and Engineering Progress*, *16*(4), 6580. https://doi.org/10.14416/j.asep.2023.01.001

[3] Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, *13*(9), 5700. https://doi.org/10.3390/app13095700

[4] Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

[5] Woods, N., & Siponen, M. (2024). How memory anxiety can influence password security behavior. *Computers & Security*, *137*, 103589. https://doi.org/10.1016/j.cose.2023.103589

[6] Daoud, A., & Dubhashi, D. (2023). Statistical modeling: The three cultures. *Harvard Data Science Review*, *5*(1), 1–51. https://doi.org/10.1162/99608f92.89f6fe66

[7] Rudin, C., Chen, C., Chen, Z., Huang, H., Semenova, L., & Zhong, C. (2022). Interpretable machine learning: Fundamental principles and 10 grand challenges. *Statistics Surveys*, *16*, 1–85. https://doi.org/10.1214/21-SS133

[8] Sen, A., Smith, G., & van Note, C. (2022). Statistical significance versus practical importance in information systems research. *Journal of Information Technology*, *37*(3), 288–300. https://doi.org/10.1177/02683962211062236

[9] Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413. https://doi.org/10.3390/info13090413

[10] Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/j.chbr.2021.100165

[11] Lee, C. S., & Chua, Y. T. (2024). The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093

[12] Tian, X. (2025). Unraveling the dynamics of password manager adoption: A deeper dive into critical factors. *Information and Computer Security*, *33*(1), 117–139. https://doi.org/10.1108/ICS-09-2023-0156

[13] Nehme, A., Li, M., & Warkentin, M. (2024). Adaptive and maladaptive factors behind password manager use: A hope-extended protection motivation perspective. *Computers & Security*, *144*, 103941. https://doi.org/10.1016/j.cose.2024.103941

[14] Alajarmeh, N., & Ladner, R. E. (2025). Password managers use among individuals who are visually impaired: Awareness, adoption, and rejection. *International Journal of Human-Computer Interaction*, *41*(10), 6318–6334. https://doi.org/10.1080/10447318.2024.2376356

[15] Mersinas, K., Bada, M., & Furnell, S. (2025). Cybersecurity behavior change: A conceptualization of ethical principles for behavioral interventions. *Computers & Security*, *148*, 104025. https://doi.org/10.1016/j.cose.2024.104025

[16] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

[17] Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

[18] Pinheiro, C., Guerreiro, S., & Mamede, H. S. (2024). A survey on association rule mining for enterprise architecture model discovery. *Business & Information Systems Engineering*, *66*(6), 777–798. https://doi.org/10.1007/s12599-023-00844-5

[19] Xue, L., Rashid, A. M., & Ouyang, S. (2024). The unified theory of acceptance and use of Technology (UTAUT) in higher education: A systematic review. *Sage Open*, *14*(1), 21582440241229570. https://doi.org/10.1177/21582440241229570

[20] Tamilmani, K., Rana, N. P., Wamba, S. F., & Dwivedi, R. (2021). The extended unified theory of acceptance and use of technology (UTAUT2): A systematic literature review and theory evaluation. *International Journal of Information Management*, *57*, 102269. https://doi.org/10.1016/j.ijinfomgt.2020.102269

[21] Jiang, J., Ma, J., Huang, X., Zhou, J., & Chen, T. (2024). Extend UTAUT2 model to analyze user behavior of China Construction Bank mobile app. *Sage Open*, *14*(4), 21582440241287070. https://doi.org/10.1177/21582440241287070

[22] Kittinger, L., & Law, V. (2024). A systematic review of the UTAUT and UTAUT2 among K-12 educators. *Journal of Information Technology Education: Research*, *23*, 17. https://doi.org/10.28945/5246

[23] Or, C. C. P. (2023). Examining unified theory of acceptance and use of technology 2 through meta-analytic structural equation modelling. *Journal of Applied Learning & Teaching*, *6*(2), 283–293. https://doi.org/10.37074/jalt.2023.6.2.7

[24] Wu, C., & Lim, G. G. (2024). Investigating older adults users' willingness to adopt wearable devices by integrating the Technology Acceptance Model (UTAUT2) and the Technology Readiness Index theory. *Frontiers in Public Health*, *12*, 1449594. https://doi.org/10.3389/fpubh.2024.1449594

[25] Sowan, B., Zhang, L., Matar, N., Zraqou, J., Omar, F., & Alnatsheh, A. (2025). A novel lift adjustment methodology for improving association rule interpretation. *Decision Analytics Journal*, *15*, 100582. https://doi.org/10.1016/j.dajour.2025.100582

[26] He, Z., Davila, D., Bi, S., Wang, T., & Hou, T. (2025). Machine learning for cybersecurity: A survey of applications, adversarial challenges, and future research directions. *Electronics*, *14*(23), 4563. https://doi.org/10.3390/electronics14234563

[27] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. *Annals of Data Science*, *10*(6), 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

[28] Podsakoff, P. M., Podsakoff, N. P., Williams, L. J., Huang, C., & Yang, J. (2024). Common method bias: It's bad, it's complex, it's widespread, and it's not easy to fix. *Annual Review of Organizational Psychology and Organizational Behavior*, *11*, 17–61. https://doi.org/10.1146/annurev-orgpsych-110721-040030

[29] Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information security behavior in health information systems: A review of research trends and antecedent factors. *Healthcare*, *10*(12), 2531. https://doi.org/10.3390/healthcare10122531

How to Cite: Jarupunphol, P., & Jeennoo, S. (2026). An Integrated UTAUT, Machine Learning, and Association Rule Mining Analysis of Password Security Behavior Among Educational Personnel. *Journal of Data Science and Intelligent Systems*. https://doi.org/10.47852/bonviewJDSIS620210144