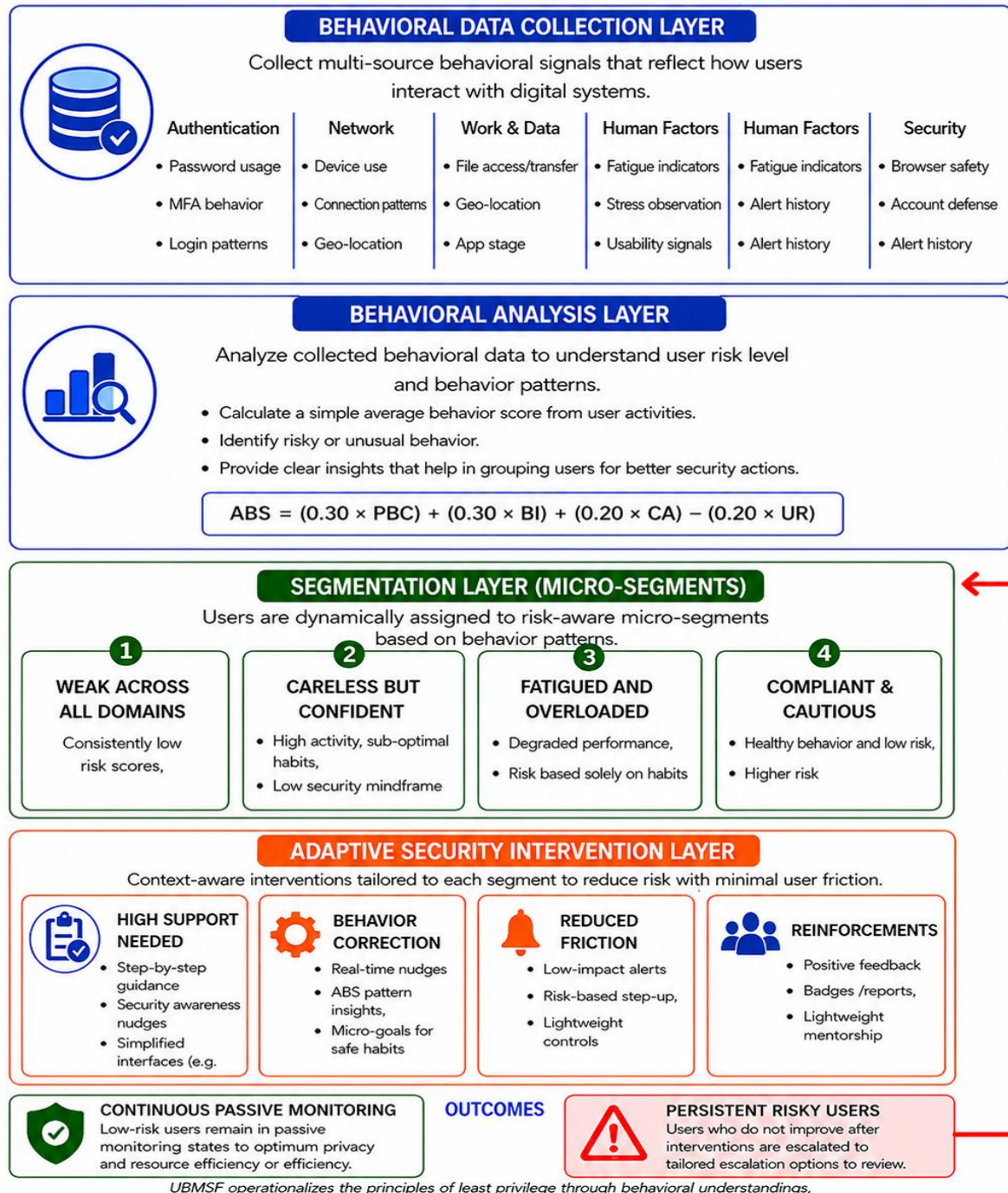


Appendix I Figures and tables

Figure 1. User Behavior Micro-segmentation framework

USER BEHAVIOR MICRO-SEGMENTATION FRAMEWORK (UBMSF)

A risk-adaptive framework that converts behavioral signals into actionable security interventions through micro-segmentation and continuous feedback.



Tables

Table 1. Cybersecurity Behavioral Performance (n = 216)

Behavioral Domain	M	SD	N	Interpretation
Password management	3.78	0.82	216	Moderate–High
Safe browsing & email vigilance	3.64	0.76	216	Moderate
Device configuration & updates	3.52	0.88	216	Moderate
Secure file handling	3.47	0.81	216	Moderate
Network usage (Wi-Fi security)	3.33	0.93	216	Moderate
Incident response & reporting	3.21	0.85	216	Moderate–Low

Table 2. Correlations among Usability, Digital Fatigue, and Cybersecurity Behavior

Variables	1	2	3
1. Usability difficulty	—		
2. Digital fatigue	0.54**	—	
3. Cybersecurity behavior	−0.46**	−0.41**	—

Note. $p < .01$. Negative correlations indicate that higher usability difficulty and fatigue correspond to lower secure behavior levels.

Table 3. Multiple Regression Predicting Cybersecurity Behavior from Usability Difficulty and Digital Fatigue

Predictor	B	SE B	β	t	p
Constant	4.11	0.18	—	22.83	< .001
Usability difficulty	−0.32	0.07	−0.39	−4.57	< .001
Digital fatigue	−0.27	0.06	−0.34	−4.18	< .001

Framework Summary: $R^2 = 0.37$, $F(2, 213) = 63.12$, $p < .001$.

Table 4. Regression Framework Predicting Cybersecurity Behavior Based on TPB Constructs

Predictor	β	SE	t	p
Perceived Behavioral Control	0.393	0.071	5.54	< .001
Subjective Norm	0.273	0.082	3.33	< .01
Behavioral Intention	0.180	0.087	2.07	< .05
Attitude	0.162	0.078	2.08	< .05

Framework Summary: $R^2 = 0.554$, $F(4,195) = 36.45$, $p < .001$.

Table 5. Behavioral Cluster Profiles (K-means output)

Cluster	Label	Dominant Traits	Proportion
1	Resilient Users	High control, low fatigue, consistent secure habits	38%
2	Overextended Users	Moderate control, high fatigue, inconsistent practices	42%
3	At-Risk Users	Low control, high usability barriers, poor response	20%

Table 6. Regression Framework Predicting Cybersecurity Behavior from Usability and Cognitive Load

Predictor	β	SE	t	p
Usability Difficulty	0.421	0.069	5.10	< 0.001
Cognitive Load	-0.357	0.084	-4.25	< 0.001

Framework Summary: $R^2 = 0.496$, $F(2, 197) = 27.36$, $p < 0.001$.

Table 7. Correlation between Digital Fatigue and Risky Behavior Indicators

Variable	r	p
Digital Fatigue – Risky Behavior	0.62	< 0.001
Digital Fatigue – Usability Difficulty	0.48	< 0.001
Digital Fatigue – Cognitive Load	0.52	< 0.001

Table 8. Operational Segmentation Rules and Thresholds

Segment	Operational Rule (Classification Logic)	Key Interpretation / Implication
Weak-Across-All-Domains	$BD_{avg} \leq 2.6$ AND $PBC \leq 2.6$ AND $US \geq 3.5$	Low capability + high usability barriers → requires guided support and simplified security tasks
Careless-but-Confident	$PBC \geq 3.5$ AND Browser Score ≤ 2.5	High confidence but risky browsing → needs behavioral nudges, phishing simulations and awareness targeting optimistic bias
Fatigued-and-Overloaded	$FD \geq 67\text{th percentile}$ AND BD_{avg} between 2.6 and 3.4	Performance drops under fatigue → use fatigue-aware prompting, reduce interruptions, schedule security tasks
Compliant-and-Cautious	$BD_{avg} \geq 3.5$ AND $PBC \geq 3.5$ AND $US \leq 2.5$	High competence and stable secure habits → can act as champions/peer mentors

Note: BD_{avg} = Behavioral domain average score; PBC = perceived Behavioral Control; US = usability difficulty score; FD = digital fatigue score.

Table 9. Evidence-to-Design Requirements Mapping for the Micro-Segmentation Framework

Evidence source	Empirical finding / justification	Design requirement	Framework feature / implementation
Behavior domain means (Table 1)	Domain performance varies	Profiling must be multi-dimensional	Segmentation uses BDavg + domain-specific triggers
TPB regression (Table 4)	PBC strongest predictor	Integrate user confidence/control into segmentation	Include PBC in rule set
Usability regression (Table 3)	Usability predicts behavior	Reduce cognitive friction	Simplified security flows
Cognitive load regression	Cognitive load reduces behavior	Lower security burden	Reduce prompts/authentication steps
Fatigue correlations (Table 7)	Fatigue linked to risky behavior	Implement fatigue-aware controls	Scheduling rules
Qualitative Theme 1	Authentication overload	Improve usability	Simplified login flows
Qualitative Theme 2	Vigilance drops late	Reduce non-urgent prompts	Dynamic segmentation
Qualitative Theme 3	Overconfidence despite risky browsing	Address optimistic bias	Simulated phishing/nudges
Qualitative Theme 4	Training quickly forgotten	Continuous practical training	Segment-tailored training
Qualitative Theme 5	Shared devices/unstable environments	Default-safe options	Device hardening policies
Qualitative Theme 6	Segmentation acceptable if privacy respected	Transparency/governance	Privacy safeguards

Table 10. Operational Logic of the Average Behavioral Score (ABS) in the Segmentation Engine

Step	Purpose	Analytical Role
1. Collect behavior scores	Get data for each domain (1–5 Likert)	Inputs from validated instrument
2. Compute Average Behavioral Score (ABS)	Summarise domains into one metric	Creates behavior fingerprint
3. Feed ABS into Segmentation Engine	Combine ABS with contextual factors	Enables data-driven grouping
4. Produce behavioral segments	Identify four user types	Supports targeted interventions

Table 11. User Segmentation Logic

Segment	Dominant Traits	Indicative Interventions
Weak-Across-All-Domains	Low capability, high usability barriers	Simplified authentication, guided support, practical training
Careless-but-Confident	High perceived control, risky online habits	Just-in-time tips, simulated phishing, browser prompts
Fatigued-and-Overloaded	Moderate skill, high digital fatigue	Fatigue-aware scheduling, reduced prompts
Compliant-and-Cautious	Consistently secure behavior, high motivation	Peer mentorship, advanced awareness updates