Human Factors Shaping Cybersecurity Behavior in Work from Home Environment in Ugandan Universities

Atuhe Aarone Mike[1]*, Akampurira Paul[2] Dr. Richard Ntwari[3]

[1,3]Department of Computer Science, Mbarara University of Science and Technology, Uganda

[2]Department of Computing, Kampala International University, Uganda

DOI: https://dx.doi.org/10.51584/IJRIAS.2026.110100125

Received: 25 January 2025; Accepted: 30 January 2026; Published: 19 February 2026

ABSTRACT

The shift to remote and hybrid work in Ugandan universities exposed new cybersecurity risks shaped by human motivation, cognitive load, and system usability challenges. As academic operations increasingly depended on digital platforms, understanding how individuals formed and enacted protective intentions within home-based work environments became critical.

This study examined how human and contextual factors—including threat perception, coping appraisal, usability difficulty, cognitive load, and digital fatigue—influenced cybersecurity behaviour among staff working remotely in Ugandan universities. Guided by the Protection Motivation Theory (PMT) and supported by constructs from the Theory of Planned Behaviour (TPB), the research adopted a sequential explanatory mixed-methods design. The quantitative phase identified key motivational and contextual predictors, while the qualitative phase explored how fatigue, usability barriers, and environmental conditions shaped protective motivation. Integration was achieved through narrative comparison and joint display analysis.

Quantitative findings revealed that coping confidence and usability difficulty were the most influential determinants of secure behaviour, whereas fatigue and cognitive load significantly undermined protective intentions. Qualitative narratives reinforced these patterns, highlighting themes of threat awareness, usability frustration, motivational fatigue, and uneven institutional support.

The study concluded that cybersecurity behaviour in remote academic environments was driven by motivational and contextual dynamics rather than technical controls alone. Strengthening coping efficacy, reducing usability burdens, and addressing digital fatigue were identified as essential strategies for developing adaptive, human-centred cybersecurity interventions in higher education.

Keywords: Cybersecurity behavior, human factors, usability, digital fatigue, Theory of Planned Behavior, work from home.

INTRODUCTION

Cybersecurity within higher education institutions has evolved into a critical research concern as digital systems increasingly support teaching, administration, and research(Armas & Taherdoost, 2025). The term *cybersecurity behaviour* in this study refers to the observable actions, decisions, and habits individuals exhibit when protecting digital assets from threats(Mattioli et al., 2023). These behaviours, ranging from password management to incident reporting, reflect how users translate awareness into secure or insecure practices within online environments (Panc, 2023).

The urgency of this topic arises from the rapid transition to remote and hybrid work arrangements following the COVID-19 pandemic, which fundamentally altered institutional technology use (Battisti et al., 2022).

While remote work improved continuity and flexibility, it simultaneously expanded exposure to cyber threats due to insecure networks, shared devices, and reduced institutional oversight. In universities, the effectiveness of cybersecurity depends not only on technical safeguards but also on human behaviour, especially under remote conditions where institutional controls are weaker(Afolalu & Tsoeu, 2025; Colabianchi et al., 2025).

Globally, research has consistently shown that users remain one of the most significant vulnerabilities in cybersecurity ecosystems. Studies in developed contexts further indicate that awareness campaigns and technical policies alone rarely guarantee secure behaviour (Armas & Taherdoost, 2025; Singh et al., 2025; Taherdoost, 2022).

Regionally, African universities face similar behavioural challenges, often compounded by infrastructure limitations and usability barriers (M. E. Eltahir & Ahmed, 2023; Mohd. E. Eltahir & Ahmed, 2023; N. Kabanda, 2025). In Uganda, local studies such as (Mirembe et al., 2025) identified gaps in digital readiness but offered limited analysis of how usability, fatigue, and behavioural control interact to shape security actions during remote work

This study examined how respondents in Ugandan higher education institutions formed and acted upon their protective motivations when working remotely. Drawing on Protection Motivation Theory (PMT), the research interprets cybersecurity behaviour as a product of users' threat appraisals, how serious and likely they perceive cyber risks to be, and coping appraisals, their confidence in managing those risks effectively. This perspective extends existing behavioural frameworks by explaining how fatigue, usability barriers, and environmental constraints alter these motivational processes, shaping the likelihood of adopting secure behaviours in remote work environments.

The objective of the study was: to assess how human, contextual, and institutional factors determine cybersecurity behavior among work from home users in Ugandan universities.
Specifically, the study addresses the following research questions:

1. What is the level of cybersecurity behavior across different domains among remote respondents?
2. Which human factors significantly predict secure or insecure behavior?
3. How do qualitative narratives explain the variations in cybersecurity practices?
4. How can findings inform the design of adaptive, user-centred cybersecurity interventions?

METHODS

Research Design and Approach

This study adopted a Sequential Explanatory Mixed-Methods Design to provide a comprehensive understanding of cybersecurity behavior among respondents. The design involved two phases: a quantitative phase to identify behavioral patterns and determinants, followed by a qualitative phase to interpret and explain those patterns. This approach enabled triangulation of statistical findings with participant narratives, ensuring both breadth and depth of analysis.

Theoretical Framework

The study was guided by the Theory of Planned Behavior (TPB), which posits that behavior is determined by attitude, subjective norms, and perceived behavioral control (PBC). Within this framework, PBC represents individuals' confidence in their ability to perform secure actions, attitude reflects personal evaluation of cybersecurity importance, and subjective norms denote social pressure to comply with security practices.

To strengthen explanatory power, the model was extended to include usability difficulty, cognitive load, and digital fatigue—human factors that influence behavioral consistency, especially in remote work environments. In addition, the Protection Motivation Theory (PMT) was incorporated to capture the motivational processes that underlie protective behavioural intentions. PMT complements TPB by introducing the threat- and coping-appraisal dimensions that motivate individuals to adopt protective actions in response to perceived risks. Integrating these perspectives provides a more comprehensive explanation of how users form, evaluate, and act upon cybersecurity intentions in remote work environments.

Figure 1: Integrated conceptual model linking PMT, TPB, usability, fatigue and cybersecurity behaviour in WFH

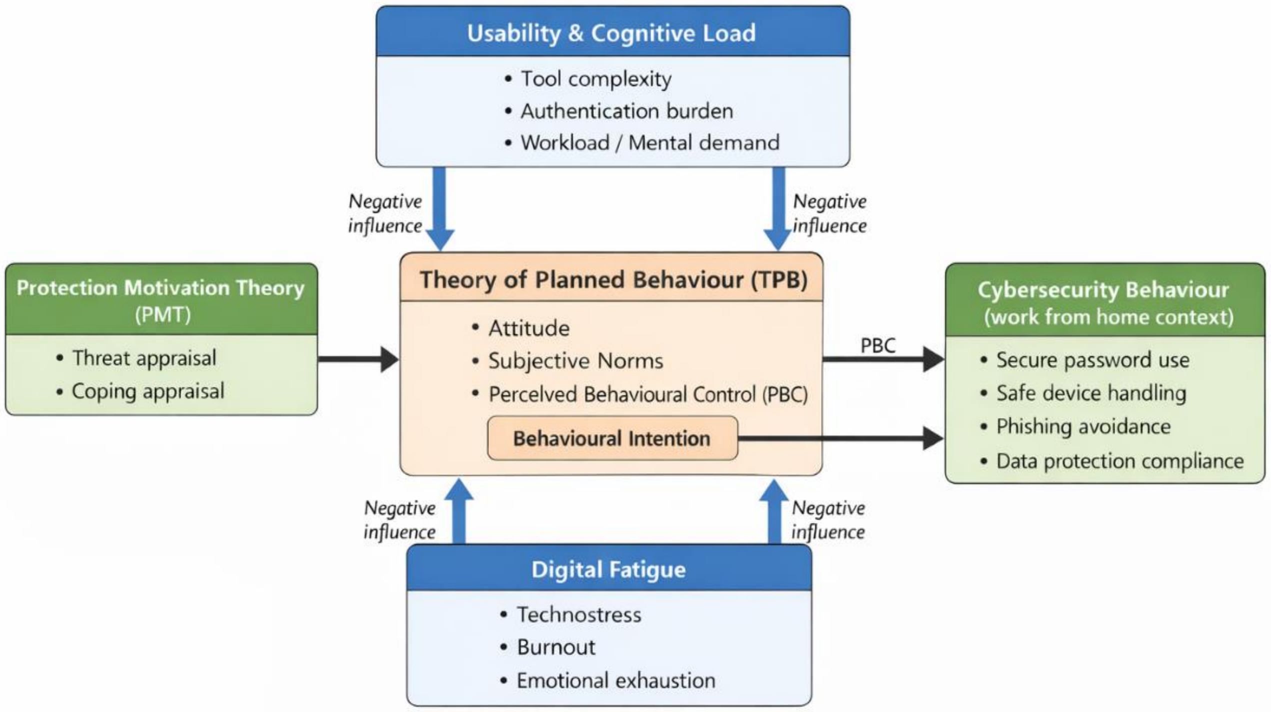

Figure 1: Integrated conceptual model linking PMT, TPB, usability, fatigue and cybersecurity behaviour in work from home contexts

Figure 1 summarises the integrated theoretical lens used in this study, linking PMT and TPB constructs to cybersecurity behaviour in remote work. PMT components (threat and coping appraisal) and TPB components (attitude, subjective norms, PBC) jointly influence behavioural intention and actual cybersecurity behaviour.

Usability barriers, cognitive load and digital fatigue are included as contextual human factors that weaken behavioural consistency by reducing motivation, perceived control and sustained compliance during remote work.

Study Setting and Participants

The study was conducted in selected Ugandan higher education institutions, including both public and private universities. Respondents comprised academic staff, administrative personnel, and students who were working or studying remotely during and after the COVID-19 pandemic.

Participants were purposively selected to represent a range of roles, departmental affiliations, and technological experiences. A total of 216 respondents participated in the quantitative phase, followed by a subset engaged in qualitative interviews. The diverse sampling approach ensured that findings reflected variations in institutional context and digital access levels.

Data Collection Procedures

Quantitative Phase

Data were collected using a validated cybersecurity behavior questionnaire designed to measure six behavioral domains—password management, safe browsing, email security, device protection, incident reporting, and network safety. The instrument also incorporated TPB constructs (attitude, subjective norms, PBC) and human factors (usability, cognitive load, fatigue), measured on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). Reliability was confirmed with Cronbach's $\alpha = 0.90$, indicating excellent internal consistency. Sampling adequacy was validated through Kaiser-Meyer-Olkin (KMO) = 0.894 and Bartlett's test of sphericity ($p < 0.001$), confirming suitability for factor analysis.

Qualitative Phase

After quantitative analysis, qualitative data were collected through open-ended survey items and semi-structured interviews. These explored participants' lived experiences, emotional responses, and contextual challenges related to cybersecurity practices during remote work. **Qualitative sample size and saturation.** The qualitative phase was conducted to evaluate the proposed usable cybersecurity framework through expert and user-informed feedback.

A total of **16 respondents** participated in the qualitative framework evaluation. Sampling and data collection progressed iteratively until **thematic saturation** was achieved, defined as the point at which no substantively new codes, themes, or framework improvement suggestions emerged from additional responses. Saturation was observed in the later interviews, where responses increasingly confirmed already-identified themes, indicating sufficient coverage of perspectives for framework validation.

To enhance credibility, qualitative coding was conducted systematically and themes were cross-checked against the framework constructs for consistency and completeness. Responses were transcribed and subjected to thematic analysis, involving:

1. Initial coding – identification of meaningful phrases and recurring ideas,

2. Pattern coding – grouping of similar ideas into broader categories, and

3. Theme development – synthesis of final themes representing dominant human factors.

Data Analysis and Integration

Quantitative data were analysed using descriptive statistics, correlation tests, and multiple regression to examine relationships among behavior, usability, fatigue, and PBC. Qualitative data were analysed using thematic procedures, and integration occurred through narrative weaving, joint display matrices, and triangulation.

These ensured that qualitative explanations aligned with quantitative results, thereby enhancing construct validity. Ethical approval was obtained from the relevant institutional review bodies. All respondents provided informed consent, and data confidentiality was maintained throughout the study.

Description of findings

The study assessed cybersecurity behavior across multiple domains and identified key human and contextual predictors influencing secure practices among remote respondents in Ugandan universities.

Cybersecurity Behavior Across Domains

Quantitative results indicated moderate overall cybersecurity behavior, with notable variations between domains. Respondents exhibited strong practices in email and network security, but weaker performance in password management and incident reporting.

Table 1. Behavioral Domain Results (n = 200)

Cybersecurity Domain	Mean Score	Interpretation
Password Management	3.5	Moderate; improvement needed for stronger practices.
Device Protection	3.7	Relatively consistent compliance across respondents.
Email and Phishing Awareness	4.0	High awareness; regular training effective.
Internet Browsing Safety	3.4	Moderate; unsafe links and downloads still common.
Incident Reporting	3.2	Low; underreporting due to uncertainty or fear.
Network Security	4.1	Strong adherence to VPN and access controls.

Overall, respondents demonstrated moderate cybersecurity behavior with stronger adherence to institutionalised security practices and weaker compliance in self-managed behaviors such as password creation and reporting incidents.

Protection Motivation Theory (PMT) constructs

Quantitative results indicate that respondents' secure cybersecurity behaviour was more strongly associated with **coping appraisal** indicators (perceived capability and support) than with **threat appraisal** alone. Participants reporting higher confidence in their ability to manage cyber risks demonstrated more consistent secure practices, while reduced behavioural consistency was observed where usability barriers and fatigue were prominent.

Respondents who reported both strong threat recognition and high coping confidence maintained comparatively higher levels of secure behaviour during work-from-home arrangements. These PMT-related patterns were further reflected in usability and workload predictors, as detailed below.

Usability and Cognitive Load

Usability challenges had a strong influence on cybersecurity behaviour ($\beta = 0.421$, $p < 0.001$). When login processes were complicated, interfaces were unclear, or systems responded slowly, users became frustrated and were more likely to take shortcuts, such as reusing passwords.

Cognitive load also showed a negative effect ($\beta = -0.357$, $p < 0.001$), indicating that higher mental strain reduced users' ability to remain alert to security risks and follow secure practices.

Regression model fit and effect size reporting

To complement the usability-specific regression estimates, a TPB-based regression model was fitted to report standardised effect sizes and overall model fit. To strengthen interpretability, regression model fit indices and standardised effect sizes were explicitly reported.

The multiple regression model predicting cybersecurity behaviour from core TPB constructs demonstrated strong explanatory power (**R = 0.744; R² = 0.554; Adjusted R² = 0.545**), indicating that approximately **55.4%** of the variance in cybersecurity behaviour was explained by the predictors. The model was statistically significant (**F(4, 210) = 65.092, p < 0.001**).

Standardised coefficients showed that **Perceived Behavioural Control (β = 0.393, p < 0.001)** exerted the strongest influence on cybersecurity behaviour, followed by **Subjective Norms (β = 0.273, p < 0.001)**, **Behavioural Intention (β = 0.180, p = 0.002)**, and **Cybersecurity Attitudes (β = 0.162, p = 0.005)**.

Table 2: Regression model fit indices and standardised effect sizes

Dependent variable: Cybersecurity behaviour

	B	SE	β (standardised)	t	p
Constant	45.411	7.876	—	5.765	<0.001
Cybersecurity attitudes	1.527	0.544	0.162	2.809	0.005
Subjective norms	2.614	0.498	0.273	5.249	<0.001
Perceived behavioural control	3.302	0.438	0.393	7.546	<0.001
Behavioural intention	1.643	0.525	0.180	3.130	0.002

Model fit indices: R = 0.744; R² = 0.554; Adjusted R² = 0.545; F(4, 210) = 65.092, p < 0.001; Std. Error of estimate = 27.715.

Digital Fatigue

Correlation analysis showed that digital fatigue was strongly linked to risky cybersecurity behaviour (r = 0.62). Respondents who spent long hours in front of screens and managed heavy digital workloads reported delaying system updates, ignoring security alerts, or reusing passwords.

These findings are consistent with Johnson and Warkentin (2021), who showed that fatigue reduces users' ability to maintain consistent cyber hygiene over time.

Environmental and Contextual Factors

Environmental variability, such as unreliable internet connectivity, limited ICT support, and domestic distractions, further constrained secure behavior. Respondents working from shared spaces or unstable connections faced higher risk exposure. Leadership support and peer influence moderately enhanced compliance but were inconsistently applied across institutions.

Table 3: Environmental and Contextual Factors

Environmental Indicator	Mean Score	Interpretation
Internet Reliability	3.6	Moderate; outages disrupt updates
ICT Support Responsiveness	3.2	Delays prompt risky workarounds
Access to Security Tools	3.4	Uneven between departments
Policy Enforcement	3.1	Fair; inconsistently applied
Home Environment Distractions	2.8	High distraction levels
Leadership Support	3.3	Improves compliance marginally
Peer Influence	3.5	Encourages modelling of good practices

Qualitative Insights

Thematic analysis revealed four dominant themes:

1. Usability Frustration – Participants found login processes and security tasks cumbersome, leading to avoidance behaviors.
2. Fatigue and Overload – Continuous screen exposure caused lapses in attention and diminished compliance.
3. Confidence and Control – Respondents who perceived higher capability managed risks more effectively.
4. Institutional Gaps – Limited technical support and usability issues weakened behavioral consistency.

These themes illuminate *why* secure behavior was inconsistent, emphasizing that behavioral lapses often stem from human limitations rather than ignorance or negligence.

Integrated Findings

This section integrates quantitative results with qualitative insights to explain differences in cybersecurity behaviour during work-from-home arrangements. While quantitative findings highlight the role of perceived behavioural control, subjective norms, behavioural intention and usability burden, qualitative narratives clarify how tool friction, workload pressure and fatigue undermine sustained compliance. The integrated evidence suggests that staff do not behave uniformly; instead, distinct behavioural segments emerge based on capability, motivation and contextual constraints.

Table 4: Integration of quantitative and qualitative data on four behavioral segments:

Segment	Behavioral Profile	Risk Level	Key Drivers of Vulnerability
1. Weak Across All Domains	Low confidence and poor performance	Very High	Usability difficulty, low PBC

2. Careless but Confident	Skilled but inconsistent	High	Overconfidence, habitual shortcuts
3. Fatigued and Overloaded	Moderate skills but lapses under strain	Moderate–High	Fatigue, workload pressure
4. Compliant and Cautious	Consistent secure behavior	Low	Awareness, supportive environment

These behavioural segments indicate that human-centred cybersecurity interventions should be tailored to user profiles rather than applied uniformly across all university staff.

This segmentation shows that cybersecurity vulnerability does not arise from technical weaknesses alone, but from the interaction between human behavior and contextual conditions. Users become vulnerable for different reasons, including low confidence, overconfidence, fatigue, or environmental pressure. The key contribution of this study lies in linking behavioral segmentation with usability and digital fatigue, providing a practical and user-centred approach to cybersecurity management within Ugandan universities.

The behavioral patterns identified in this study are consistent with the segmentation logic implemented in the User-Behaviour Micro-Segmentation Framework (UBMSF) described in earlier work (Author, 2026b). That framework translates the empirical findings presented here into a structured model designed to support targeted cybersecurity interventions. In the present paper, the UBMSF is referenced only to contextualise these behavioral insights, while its detailed architecture and validation are reported in the related framework publication.

DISCUSSION

This study examined how human, contextual, and institutional factors shape cybersecurity behaviour in work-from-home environments within Ugandan universities. By integrating PMT and the TPB, the findings extend existing cybersecurity literature by demonstrating that secure behaviour in remote academic settings is driven less by awareness or policy compliance and more by users' motivational capacity, usability experiences, and levels of digital fatigue.

Cybersecurity Behaviour and Domain-Level Variations

The finding of moderate overall cybersecurity behaviour, with stronger performance in institutionalised practices (email and network security) and weaker performance in self-managed behaviours (password management and incident reporting), aligns with prior studies in higher education contexts. Previous research has shown that behaviours embedded within automated or centrally enforced systems tend to achieve higher compliance than those requiring sustained individual effort and judgment (Afolalu & Tsoeu, 2025; Oroni & Xianping, 2025; Ramamurthy et al., 2025).

Consistent with findings from African higher education institutions (Aloyce Semlambo, 2025; Mbonimpa et al., 2024; Okanda & Abass, 2025), incident reporting remained particularly weak. Participants' uncertainty about reporting procedures and fear of blame reflect broader organisational culture challenges documented in cybersecurity behaviour research, where reporting is often perceived as risky rather than protective. This reinforces the argument that cybersecurity behaviour is socially and institutionally mediated, not merely knowledge-based.

Role of Coping Appraisal and Perceived Behavioural Control

One of the most significant findings was that coping confidence and Perceived Behavioral Control (PBC) were the strongest predictors of secure behaviour. This result strongly supports both PMT and TPB assumptions, confirming that users who believe they are capable of responding effectively to cyber threats are more likely to engage in protective actions. This aligns with prior studies showing that self-efficacy and perceived control consistently outperform threat awareness alone in predicting cybersecurity (Al-Shanfari et al., 2022; Ghazi et al., 2025; William Vortia, 2025). Importantly, this study extends those findings by demonstrating that in remote work environments, PBC is highly sensitive to usability barriers and fatigue. Even when users recognise cyber threats as serious, their protective motivation diminishes if systems are perceived as difficult to use or cognitively demanding. This finding challenges awareness-centric cybersecurity models and underscores the need for capability-oriented interventions.

Usability Difficulty and Cognitive Load as Behavioural Constraints

The strong negative influence of usability difficulty and cognitive load on cybersecurity behaviour is consistent with human-centred security research, which argues that complex security mechanisms often encourage risky workarounds rather than compliance (Abuiteiwi & Escobar, 2025; Al-Badayneh et al., 2025; Grobler et al., 2021; Kävrestad et al., 2024). When login processes, authentication steps, or system interfaces were perceived as cumbersome, respondents reported shortcut behaviours such as password reuse or delayed updates.

These findings corroborate earlier usability-security trade-off studies but add contextual depth by situating them within resource-constrained and remote academic environments. In contrast to studies conducted in technologically mature settings, this research shows that usability challenges in Ugandan universities are often compounded by unreliable connectivity, limited ICT support, and heterogeneous user skill levels. As a result, cognitive load becomes a critical determinant of behavioural consistency rather than a peripheral factor.

Digital Fatigue and Sustained Cybersecurity Behaviour

Digital fatigue emerged as a strong correlate of risky cybersecurity behaviour, reinforcing emerging evidence that prolonged digital engagement undermines users' capacity to maintain secure practices over time and this is in alignment with existing works like (Mizrak et al., 2025). Respondents experiencing high fatigue were more likely to ignore alerts, postpone updates, and disengage from security-related tasks.

Our study advances existing work by positioning fatigue not merely as a psychological outcome of remote work, but as a direct behavioural risk factor in cybersecurity. Unlike traditional models that assume rational and consistent user decision-making, the findings demonstrate that motivational depletion plays a critical role in security lapses. This insight is particularly relevant for higher education institutions, where extended screen time and multitasking are endemic.

Environmental and Institutional Moderation Effects

Environmental and institutional factors, including ICT support responsiveness, leadership engagement, and home working conditions, were found to moderate cybersecurity behaviour. These results align with organisational behaviour studies suggesting that supportive leadership and peer norms can reinforce secure practices, albeit inconsistently (Al-Nuaimi, 2022; Sutton & Tompson, 2025; Ye, 2025).

However, the mixed strength of these effects suggests that institutional influence alone is insufficient to compensate for poor usability or high fatigue. This finding nuances existing research by showing that while organisational support is necessary, it must be paired with system-level and motivational interventions to produce sustained behavioural change.

Behavioural Segmentation and Contribution to Existing Frameworks

The identification of four behavioural segments, ranging from "weak across all domains" to "compliant and cautious", is consistent with prior attempts to classify cybersecurity users based on risk profiles. However, this study contributes novel insight by explicitly linking segmentation to usability burden and digital fatigue, rather than solely to awareness or compliance attitudes.

By empirically grounding behavioural segmentation within PMT and TPB constructs, the findings provide a bridge between behavioural theory and practical cybersecurity management. This supports earlier calls for differentiated, user-specific interventions (Taherdoost, 2022) and (William Vortia, 2025) strengthens the

Limitations and external validity

This study was conducted within Ugandan universities operating under resource-constrained Work from Home conditions, which strengthens contextual relevance but may limit broader generalisability. The findings are therefore most applicable to comparable higher education institutions in developing-country contexts with similar ICT infrastructure constraints, workload pressures and institutional policy environments.

However, the integrated human-factor mechanisms observed—particularly the effects of perceived behavioural control, usability burden and digital fatigue—may still be transferable to other organisational settings implementing work-from-home arrangements, provided contextual adaptations are made.

CONCLUSION AND RECOMMENDATION

This study set out to determine how human, contextual, and institutional factors influence cybersecurity behavior among remote respondents in Ugandan universities. The findings revealed that cybersecurity behavior is primarily shaped by human and contextual conditions rather than technical systems alone. Perceived behavioral control, usability difficulty, cognitive load, and digital fatigue emerged as the strongest determinants of behavior, while environmental factors such as limited institutional support and unreliable infrastructure further moderated these effects.

The novelty of this study lies in its integration of behavioral psychology with usability and fatigue constructs within the context of remote higher education in a developing country. Unlike earlier research that focused solely on awareness or attitude, this study demonstrates that users' cognitive and emotional states, particularly fatigue and perceived control, play a defining role in determining secure conduct.

Furthermore, the introduction of behavioral segmentation provides an innovative framework for differentiating user risk profiles, thereby enabling institutions to design interventions tailored to distinct behavioral patterns rather than one-size-fits-all policies.

In summary, this study demonstrates that cybersecurity behaviour is driven by motivational dynamics rather than technical capability alone. Users' protective intentions fluctuate according to their perceived threats, coping confidence, and levels of digital fatigue.

Strengthening cybersecurity culture in remote academic environments therefore requires addressing the motivational fatigue that undermines users' willingness to act securely—not merely enhancing awareness or enforcing compliance policies.

The results demonstrate that:

1. Confidence and perceived capability (PBC) directly increase adherence to secure practices.
2. Usability challenges and fatigue substantially reduce compliance, especially during prolonged online engagement.
3. Environmental and institutional contexts mediate behavior by either enabling or constraining secure actions.
4. User segmentation reveals that cybersecurity vulnerability is unevenly distributed—some groups require intensive support while others act as role models for secure conduct.

   These insights collectively affirm that cybersecurity management must evolve from uniform awareness programs toward differentiated, behaviourally informed interventions.

Practical Recommendations

1. Integrate user-centred design principles in institutional systems to reduce usability friction and improve compliance.

2. Adopt fatigue-aware cybersecurity policies and workflows (e.g., automation, simplified controls, smart reminders) to reduce cognitive burden.

3. Implement continuous and task-based cybersecurity training (micro-learning and simulations) instead of one-off workshops.

4. Promote peer learning and leadership engagement to reinforce positive security norms and accountability.

5. Apply behavioural segmentation to tailor interventions for diverse user risk profiles and capacity levels.

Table 5: Practical implementation checklist for human-centred cybersecurity in WFH universities

Domain	Action (What to implement)	Responsible unit	Suggested timeframe	Expected outcome
Policy & governance	Update cybersecurity policies to explicitly include WFH practices (device use, data handling, reporting incidents, authentication standards).	University management / ICT Directorate	0–3 months	Clear compliance expectations for remote staff
Training & awareness	Deliver role-based cybersecurity training (academic staff/admin staff) with practical phishing simulations and short refreshers.	ICT + HR + Quality assurance	Quarterly	Improved threat response and safer behavior
Usability improvement	Simplify authentication and reduce user burden (SSO, password managers, MFA usability support).	ICT Directorate	3–6 months	Less resistance; higher compliance
Workload management	Adjust digital workload and meeting culture to reduce cognitive overload (avoid excessive tools/platforms).	Heads of Department / HR	0–6 months	Reduced cognitive load → improved security behaviour
Fatigue mitigation	Provide psychosocial support, digital wellness initiatives, and WFH scheduling policies.	HR + Staff welfare	0–12 months	Reduced fatigue-driven risky practices
Technical controls	Enforce endpoint protection, encryption, automatic updates, secure VPN access, and safe backups.	ICT Directorate	0–6 months	Reduced exposure to malware/data loss

Monitoring & feedback	Establish usable reporting channels (simple incident reporting, helpdesk response SLAs, feedback loops).	ICT Helpdesk	Continuous	Faster detection & response
Culture & norms	Promote leadership-driven security culture; reward secure behaviour and peer reinforcement.	University leadership	Continuous	Stronger subjective norms and shared responsibility

Table 5 presents a concise implementation checklist to support policymakers and university administrators in deploying human-centred cybersecurity interventions for work-from-home settings.

Future Research Directions

Future studies should extend this framework by:

1. Conducting experimental or longitudinal designs to measure behavioral change over time.
2. Testing fatigue-aware and usability-enhanced system prototypes in real institutional environments.
3. Exploring cross-sectoral comparisons to validate behavioral segmentation across public and private organisations.

Such efforts will deepen understanding of the dynamic relationship between human factors and cybersecurity resilience in digital education ecosystems.

REFERENCES

1. Abuiteiwi, A., & Escobar, S. (2025). Evaluating the human factor in cybersecurity threats (a Systematic Literature Review) (SSRN Scholarly Paper No. 5576064). Social Science Research Network. https://doi.org/10.2139/ssrn.5576064
2. Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. Future Internet, 17(12), 575.
3. Al-Badayneh, D., AL-BADAYNEH, D., & HASHISH, R. (2025). Human Factors of Cybersecurity. Journal of Posthumanism, 5. https://doi.org/10.63332/joph.v5i4.1242
4. Al-Nuaimi, M. (2022). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: A systematic review. Global Knowledge, Memory and Communication, 73. https://doi.org/10.1108/GKMC-12-2021-0209
5. Aloyce Semlambo, A. (2025). Behavioral, Organizational and Cultural Determinants of ICT Security Incident Reporting in Tanzanian Public Higher Learning Institutions. EAST AFRICAN JOURNAL OF EDUCATION AND SOCIAL SCIENCES, 6(4), 79–87. https://doi.org/10.46606/eajess2025v06i04.0457
6. Al-Shanfari, I., Mohamed, W., Tabook, N., Ismail, R., & Ismail, A. (2022). Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees. International Journal of Advanced Computer Science and Applications, 13, 479–490. https://doi.org/10.14569/IJACSA.2022.0130855
7. Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. Information, 16(5), 336.
8. Battisti, E., Alfiero, S., & Leonidou, E. (2022). Remote working and digital transformation during the COVID-19 pandemic: Economic–financial impacts and psychological drivers for employees. Journal of Business Research, 150, 38–50.

9. Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. Journal of Innovation & Knowledge, 10(3), 100695. https://doi.org/10.1016/j.jik.2025.100695
10. Eltahir, M. E., & Ahmed, O. S. (2023). Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan. Information Sciences Letters, 12(1), 171–183. https://doi.org/10.18576/isl/120113
11. Ghazi, K. M. A., Ahmed El-Said, O., Ahmad Rather, R., & Elbayoumi Salem, I. (2025). Extrinsic and intrinsic motives to boost employee cybersecurity behavior and organisational cyber-resilience in hotels: Mediation and moderation analysis. Journal of Hospitality and Tourism Technology, 17(1), 250–273. https://doi.org/10.1108/JHTT-05-2024-0310
12. Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. Frontiers in Big Data, 4, 583723. https://doi.org/10.3389/fdata.2021.583723
13. Kävrestad, J., Rambusch, J., & Nohlberg, M. (2024). Design principles for cognitively accessible cybersecurity training. Computers & Security, 137, 103630. https://doi.org/10.1016/j.cose.2023.103630
14. Mattioli, R., Malatras, A., Hunter, E. N., Biasibetti Penso, M. G., Bertram, D., & Neubert, I. (2023). Identifying emerging cyber security threats and challenges for 2030. European Union Agency for Cybersecurity (ENISA), Athens-Heraklion, Greece, 64.
15. Mbonimpa, T., Richard, N., Innocent, M. J., & Priscilla, M. (2024). Investigating Security Awareness and Incident Reporting levels at Mbarara University of Science and Technology. Indonesian Journal of Innovation and Applied Sciences (IJIAS), 4(3), 208–216. https://doi.org/10.47540/ijias.v4i3.1482
16. Mirembe, D. P., Kibukamusoke, M., Mutebi, R., & Namagembe, B. (2025). Remote Working Trends and Their Impact on Employee Performance and Organizational Productivity in Uganda. Science, Technology & Public Policy, 9(1), 47–62. https://doi.org/10.11648/j.stpp.20250901.15
17. Mizrak, F., Demirel, H. G., Yaşar, O., & Karakaya, T. (2025). Digital detox: Exploring the impact of cybersecurity fatigue on employee productivity and mental health. Discover Mental Health, 5(1), 25. https://doi.org/10.1007/s44192-025-00149-x
18. N. Kabanda, M. (2025). Information Security Awareness in Sub-Saharan African Schools: The Role of Educational Leadership in Turbulent Times. In M. Mohiuddin, E. Hosseini, M. Julfikar Ali, & M. Osman Gani (Eds.), Business, Management and Economics (Vol. 30). IntechOpen. https://doi.org/10.5772/intechopen.114332
19. Okanda, P., & Abass, A. (2025). AN EVALUATION OF CYBER INCIDENT MANAGEMENT SYSTEMS IN HIGHER EDUCATION INSTITUTIONS (HEIS) IN KENYA. Journal of Digital Security and Forensics, 2(2), 11–37. https://doi.org/10.29121/digisecforensics.v2.i2.2025.50
20. Oroni, C. Z., & Xianping, F. (2025). Evaluating the influence of cybersecurity policies and cybersecurity behavior on institutional security performance in remote learning: The moderating role of technological readiness. Sustainable Futures, 10, 101554. https://doi.org/10.1016/j.sftr.2025.101554
21. Panc, D. (2023). An analysis of the European Union multifaceted approach to addressing the evolving cybersecurity challenges. Conferința Internațională Educație Și Creativitate Pentru o Societate Bazată Pe Cunoaștere-DREPT, 17(XVII), 112–116.
22. Ramamurthy, V., Bogalin, V., Zvavahera, P., & Aquino, E. (2025). Evaluating cybersecurity awareness and practices among employees at a private university in Papua New Guinea. IBSUniversity Journal, 1–19.
23. Singh, K., Chatterjee, S., Mariani, M., & Wamba, S. F. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. Technovation, 143, 103219. https://doi.org/10.1016/j.technovation.2025.103219
24. Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. Computers & Security, 148, 104110. https://doi.org/10.1016/j.cose.2024.104110
25. Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. Electronics, 11(14), 2181.

26. William Vortia. (2025). Modelling cybersecurity awareness, perceived threats and secure online behavioral intentions among Ghanaian university students: A PLS-SEM Approach. Magna Scientia Advanced Research and Reviews, 14(2), 096–111. https://doi.org/10.30574/msarr.2025.14.2.0094
27. Ye, Q. (2025). Digital leadership enhances organizational resilience by fostering job crafting: The moderating role of organizational culture. Scientific Reports, 15, 24640. https://doi.org/10.1038/s41598-025-09144-2