Journal of Computer Science and Technology
[ISSN 2789-9985]
Volume: 04 Issue: 01 | July-2026
JCST

# Protective Capability as a Developmental Hierarchy: Evidence That Cyber Security Behaviours are Ordered, Not Parallel

**Authors**
**Julius Sirma [1]; Patrick K. Wamuyu [2]; Dalton Ndirangu [3]**
**Main author's email: julius.sirma@gmail.com**

**(1.2.3) United States International University-Africa.**

**Cite this article in APA**
Sirma, J., Wamuyu, P. K., & Ndirangu, D. (2026). Protective capability as a developmental hierarchy: Evidence that cyber security behaviours are ordered, not parallel. *Journal of computer science and technology, 4*(1), 74-85. https://doi.org/10.51317/jcst.v4i1.1109

OPEN ACCESS
A publication of Editon Consortium Publishing (online)

**Article history**
Received: 2026-05-18
Accepted: 2026-06-24
Published: 2026-07-31

Scan this QR to read the paper online



**Abstract**
This study aimed to determine whether protective capability is instead developmental: an ordered structure in which each stratum of competence enables the next. Research on protective cyber security behaviour has largely treated such behaviours as a parallel set of practices that users adopt independently. Using a convergent parallel mixed-methods design, four protective behaviours- foundational security hygiene, proactive defence, advanced protection, and recovery and help-seeking were modelled as an ordered structure and estimated through covariance-based structural equation modelling on survey data from 304 social media users in Kenya recruited through non-probability sampling, with corroborating evidence from ten focus-group discussions. The model demonstrated good fit, and all four hypothesised paths were supported, with coefficients strengthening toward the apex of the hierarchy. Two further results identify the structure as sequential rather than merely correlated. Adjacent-level effects were large, whereas the skip-level effect of hygiene on advanced protection was small. Additionally, the influence of hygiene on advanced protection attenuated substantially when proactive defence was controlled, indicating partial mediation through the intervening level. Protective capability transfers strongly between adjacent strata and weakly across them. A further finding qualifies the practical reading: it was the base of the hierarchy, not its apex, that predicted sustained safe participation. The results extend the coping-appraisal component of protection motivation theory by revealing that self-efficacy accumulates hierarchically and imply that security education should be sequenced rather than delivered as an undifferentiated set of practices.

**Key terms:** Cyber hygiene, cyber resilience, protective behaviour, protection motivation theory, structural equation modelling.

## 1.0 INTRODUCTION

This study aimed to determine whether protective capability is instead developmental: an ordered structure in which each stratum of competence enables the next. Digital systems users are routinely urged to adopt an assortment of protective behaviours: to choose strong passwords, to verify links, to enable two-factor authentication, to audit their privacy settings, to report suspicious accounts, to change credentials after a breach. The advice is typically delivered as a list. Its implicit assumption is that these behaviours are independent of one another, that a user may adopt any one of them without having adopted the others, and that the task of security education is therefore to increase the number of practices a user performs.

This assumption is rarely examined as research on protective security behaviour has extensively documented which behaviours users adopt, what predicts their adoption, and how adoption relates to victimisation (Ngo et al., 2026; van der Schyff & Flowerday, 2021; Dzidzah et al., 2020). However, the field has predominantly treated protective behaviours as a parallel set, entering them into models as interchangeable indicators of a single latent construct, or examining them one at a time. The question of whether they stand in a structural relation to one another, whether the capacity to perform one is conditioned on having developed the capacity to perform another, has largely gone unasked.

The question matters both theoretically and practically. Theoretically, protection motivation theory holds that protective action depends on coping appraisal: on the user's judgement that a response is efficacious and that they are capable of performing it (Szczuka et al., 2023; Tang et al., 2021). However, the theory treats coping appraisal as a property of the individual in relation to a specific threat and response, and it does not specify how the capacity to appraise and perform one response relates to the capacity to perform another. Suppose protective behaviours are ordered; suppose the self-efficacy required for sophisticated defence is built upon competence acquired through routine practice. Coping appraisal is not a single quantity but an accumulating one, and protection motivation theory requires extension accordingly.

Practically, the difference is decisive for how security education is designed. If protective behaviours are parallel, then a program should maximise coverage, teaching as many practices as time permits, in any order. If they are ordered, then a program that teaches advanced countermeasures to users who have not established foundational habits is building on an absent foundation, and coverage without sequence will fail.

This study tested the developmental proposition directly. The research objective was to determine whether four protective behaviours, foundational security hygiene, proactive defence, advanced protection, and recovery and help-seeking, form an ordered developmental structure rather than a parallel set, and, if so, to characterise the form of that ordering. Two research questions followed: first, does each stratum of protective capability significantly enable the next; and second, does capability transfer selectively between adjacent strata, the pattern that would distinguish a genuine sequence from a set of merely correlated behaviours? The study modelled the four behaviours as an ordered structure and estimated it on data from 304 social media users in Kenya, with corroborating qualitative evidence from ten focus-group discussions. The paper's contribution is threefold. It provides the first structural test, to our knowledge, of whether protective behaviours form a developmental hierarchy. It identifies an empirical signature by

which a sequential structure may be distinguished from mere correlation among behaviours. It further draws out the consequences for the theory of coping appraisal and for the design of security education.

## 2.0 LITERATURE REVIEW

### The Parallel-Practice Assumption

The prevailing treatment of protective behaviour in the security literature is as a set of parallel practices. Studies of cyber hygiene typically operationalise it as a composite of routine practices: password strength, software updating, link verification, and relate that composite to outcomes such as victimisation (Ngo et al., 2026). Studies of protective adoption model the determinants of a single behaviour, or of an undifferentiated protective index, as a function of awareness, perceived vulnerability, or self-efficacy (Debb & McClellan, 2021; Hasan et al., 2025; van der Schyff & Flowerday, 2021). Where multiple behaviours are examined, they are generally entered as reflective indicators of one latent protective construct, which presupposes that they are interchangeable manifestations of a common disposition rather than distinct competencies standing in an order.

This treatment is reasonable as a first approximation, and it has produced robust findings: awareness mediates protective adoption (van der Schyff & Flowerday, 2021; Sari et al., 2023), habit and social context shape preventive conduct (Wright et al., 2024), and training improves practice, particularly when sustained (Tóth et al., 2025; Alsulami & Dupuis, 2024).

It is crucial to acknowledge that the parallel-practice model is not merely a default assumption but a position with genuine empirical support, and a balanced review must state its strengths. Several lines of evidence are consistent with it. Studies of phishing response find that users vary in their susceptibility to individual deceptions in ways that appear specific to the threat rather than reflecting a general protective capacity, which suggests that protective responses may be somewhat independent of one another (Frauenstein, 2019; Yeng et al., 2022). Human-factors accounts likewise treat the several protective behaviours as distinct responses to distinct psychological vulnerabilities rather than as a single ordered competence (Saleem et al., 2024; Khadka & Ullah, 2025). On this view, a user may adopt two-factor authentication without having established habitual link verification, because the two behaviours address different concerns and are learned through different channels. The parallel model also has the virtue of parsimony: it requires no assumption about the order in which behaviours are acquired. The present study takes this position seriously as the competing hypothesis against which the developmental account is tested, rather than as a straw man; the question is which the data support.

### The Case for a Developmental Hierarchy

Three lines of evidence suggest that protective behaviours are ordered rather than parallel.

The first is that they systematically differ in what they demand. Foundational practices: using a strong password, hesitating before an unfamiliar link, require little technical knowledge and are near-universally recommended. Advanced practices: diversifying authentication methods, auditing application permissions, monitoring accounts for anomalous activity, require substantially more knowledge, effort, and confidence. Recovery behaviours: securing a compromised account, tracing an unauthorised transaction, navigating a platform's reporting apparatus; presuppose not only competence but the prior occurrence of an incident. Where behaviours differ this markedly in their demands, an ordering in their acquisition is plausible on its face.

The second is the coping-appraisal logic of protection motivation theory itself. Protective action requires that the user believe a response will work and that they can perform it (Szczuka et al., 2023). However, self-efficacy is not conjured; it is built through successful performance. A user who has never successfully configured a privacy setting has little basis on which to judge themselves capable of auditing application permissions. The theory's own mechanism, followed through, implies that competence at one level furnishes the self-efficacy required at the next, which is to say, it implies a hierarchy, though the theory has not been read this way.

The third is that the developmental view is increasingly implied, though seldom modelled, in recent work. Digital resilience has been characterised as a set of layered competencies acquired progressively rather than adopted at once (Naeem & Mushibwe, 2025). Studies of protective action among mobile-wallet users show that the more sophisticated behaviours are conditioned by motivation and capability in ways the basic ones are not (Ng et al., 2026). Studies on student security behaviour against phishing reveal that protective action follows the cognitively mediated appraisal logic of established behavioural models rather than being adopted at random (Gwenhure, 2025). Work on the attitude–behaviour gap in cyber resilience finds that users who hold protective intentions frequently cannot enact them, which is what a missing foundational stratum would produce (Goliath et al., 2026). That human error remains a persistent source of cyber risk even among the aware underscores why protective competence is better understood as something built cumulatively than as a set of discrete practices switched on at will (Risteski et al., 2026). The logic is widely present in the literature; the structure has not been tested.

**Conceptual Definitions**

Before specifying the hypotheses, the four constructs are conceptually defined. These include foundational security hygiene, which is the set of routine, low-effort preventive practices that require little specialised knowledge and are near-universally recommended; the use of strong and distinct passwords, habitual caution toward unfamiliar links and unsolicited requests, and basic configuration of privacy settings. Proactive defence is anticipatory practice directed at identifying deception before it succeeds: the independent verification of suspicious contacts and attentiveness to the markers of fraudulent communication. Advanced protection is demanding preventive competence requiring greater knowledge, effort, and confidence: the use of two-factor authentication, the auditing of application permissions, the blocking and reporting of malicious accounts, and the active monitoring of accounts for anomalous activity. Recovery and help-seeking, which is post-incident competence, presupposes that an incident has occurred: securing a compromised account, changing credentials, monitoring for unauthorised activity, and seeking assistance from platforms, institutions, or trusted others. These four are respectively ordered by the knowledge, effort, and prior experience they demand, from least to greatest.

**Hypotheses**

We modelled protective capability as four ordered strata and specified the paths that a developmental structure implies. Foundational security hygiene, as the base, should enable the anticipatory practices of proactive defence, and should also exert some direct influence on advanced protection. Proactive defence should enable advanced protection, which, as the most demanding preventive competence, should enable the recovery and help-seeking behaviours that presuppose it.

The hypotheses include:

H1. Foundational security hygiene positively influences proactive defence.

H2. Foundational security hygiene positively influences advanced protection.
H3. Proactive defence positively influences advanced protection.
H4. Advanced protection positively influences recovery and help seeking.

A developmental structure implies more than that these four paths are significant. However, a set of merely correlated behaviours would also produce significant paths. In turn, this implies a distinctive pattern: capability transfers strongly between adjacent strata and weakly across them, and the influence of a lower stratum on a non-adjacent higher one operates substantially through the level between them. Therefore, beyond the four hypotheses, we examined whether the effect of hygiene on advanced protection was mediated by proactive defence, and how the magnitudes of adjacent- and skip-level effects compared.

## 3.0 METHODOLOGY

The study formed part of a larger investigation employing a convergent parallel mixed-methods design. The quantitative strand surveyed 304 social media users in Kenya. Because no enumerable sampling frame exists for this population, non-probability sampling, combining purposive and convenience approaches, was used; participants were only eligible if they were aged 18 years or above and were active users of one or more of the social media platforms under study. The achieved sample was predominantly female (226; 74.3%) and young (278; 91.4% aged 18–24 years), and most respondents held or were pursuing an undergraduate degree (55.9%) or a college diploma (32.6%). The demographic concentration is a limitation, addressed in section 5.4. The adequacy of the sample was judged against established guidance for structural equation modelling: it exceeded both the minimum of 200 cases and the ratio of ten cases per estimated indicator recommended by Kline (2016), and it satisfied the widely applied criterion that a sample of 300 is adequate for factor-analytic work (Tabachnick & Fidell, 2019).

The qualitative strand comprised ten focus-group discussions of approximately ten participants each, drawn purposively from two populations of active social media users, mainly church congregations and university students. Participants were included only if they were aged 18 years or above. This was so long as they were active users of at least one platform under study, and were able to speak to personal or observed experience of social engineering; individuals who did not use social media, or who declined to consent to participation, were excluded. The two populations were purposely selected to capture a range of ages, occupations, and social contexts within the target population. Discussions were documented as structured thematic records rather than verbatim transcripts, a constraint that bounds the qualitative claims made below.

The four constructs were measured by fifteen items rated on a five-point Likert scale, derived from operational definitions established in the literature. Foundational security hygiene (4 items) captured routine preventive practice: password strength and distinctness, caution with unfamiliar links and unsolicited requests, and basic privacy configuration. Proactive defence (3 items) captured anticipatory practice: verifying suspicious contacts through independent channels and being attentive to markers of deception. Advanced protection (5 items) captured demanding preventive competence: two-factor authentication, permission auditing, blocking and reporting, and account monitoring. Recovery and help-seeking (3 items) captured post-incident action: securing compromised accounts, changing credentials, monitoring for unauthorised activity, and seeking assistance.

One item from the initial protective-behaviour pool was excluded before modelling, having returned a communality of .108 and a maximum loading of .200 in exploratory analysis.

To ensure transparency, consistency, and reliability of the analysis, data were analysed through a reproducible computational pipeline. Factorability was assessed through the Kaiser–Meyer–Olkin (KMO) measure and Bartlett's test of sphericity. Exploratory factor analysis employed oblique (Promax) rotation, the constructs being theoretically expected to correlate. Reliability and validity were assessed through Cronbach's alpha, composite reliability (CR), average variance extracted (AVE), and the Fornell–Larcker criterion. The measurement and structural models were estimated through covariance-based structural equation modelling, selected over partial least squares because the aim was confirmatory. Fit was assessed through the comparative fit index (CFI), Tucker–Lewis index (TLI), and root-mean-square error of approximation (RMSEA). Effect sizes were computed as Cohen's $f^2$. Mediation was examined by comparing the total effect of hygiene on advanced protection with its direct effect when proactive defence was controlled, estimated on unit-weighted composites. Focus-group data were analysed through reflexive thematic analysis (Braun & Clarke, 2006).

**Ethical Considerations**

The study was conducted in accordance with recognised ethical standards for research involving human participants. Participation in both strands was voluntary and based on informed consent, obtained after participants had been advised of the purpose of the study and their right to withdraw at any point without consequence. No individually identifying information was recorded in either strand as survey responses were anonymous, and focus-group contributions were documented at the level of themes rather than attributed to named individuals. Ultimately, data were stored securely and used solely for the research.

## 4.0 FINDINGS AND DISCUSSION

### Measurement Model

The data were well suited to factor analysis (KMO = .892; Bartlett's $\chi^2(105) = 1678.7$, $p < .001$). Exploratory factor analysis returned a four-factor solution corresponding to the four hypothesised constructs, accounting for 40.1 per cent of cumulative variance, with the foundational-hygiene, advanced-protection, and recovery items each loading cleanly on their own factor.

Reliability and validity statistics are reported in Table 1. Three of the four constructs met the .70 threshold for internal consistency, and proactive defence fell marginally below it ($\alpha = .656$). Composite reliability was acceptable throughout. Average variance extracted approached or met .50 for hygiene, advanced protection, and recovery, and fell below it for proactive defence. The square root of AVE exceeded each construct's inter-construct correlations in every case, supporting discriminant validity.

**Table 1: Reliability and Validity of the Four Protective-Capability Constructs (N = 304)**

| Construct | Items | α | CR | AVE | √AVE |
|---|---|---|---|---|---|
| Foundational hygiene | 4 | .767 | .776 | .466 | .683 |
| Proactive defence | 3 | .656 | .667 | .403 | .635 |
| Advanced protection | 5 | .822 | .823 | .482 | .694 |
| Recovery and help-seeking | 3 | .747 | .749 | .502 | .709 |

The confirmatory measurement model demonstrated good fit, $\chi^2(84) = 194.68$, CFI = .931, TLI = .914, RMSEA = .066. Standardized loadings ranged from .574 to .788 and were significant throughout.

**Structural Model: the Four Hypothesised Paths**

The structural model demonstrated good fit, $\chi^2(86) = 200.81$, CFI = .929, TLI = .913, RMSEA = .066. All four hypotheses were supported (Table 2).

**Table 2: Structural Path Estimates and Effect Sizes**

| H | Path | β | z | p | $f^2$ |
|---|---|---|---|---|---|
| H1 | Hygiene → Proactive defence | .531 | 5.88 | < .001 | .393 (large) |
| H2 | Hygiene → Advanced protection | .284 | 3.74 | < .001 | .088 (small) |
| H3 | Proactive defence → Advanced protection | .666 | 6.22 | < .001 | .797 (large) |
| H4 | Advanced protection → Recovery | .786 | 9.38 | < .001 | 1.616 (large) |

Two features of this pattern warrant emphasis. The first is the monotonic strengthening of the coefficients as the hierarchy ascends: from .531 at its base, through .666, to .786 at its apex. The dependence of each stratum upon the one beneath it does not merely persist as capability increases; it intensifies. Recovery and help-seeking, the most demanding behaviours and the ones presupposing an incident, are the most tightly conditioned by the competence preceding them.

The second is the contrast between the adjacent paths and the one non-adjacent path. The three adjacent-level effects are all large ($f^2$ = .393, .797, 1.616). The skip-level effect of hygiene on advanced protection is small ($f^2$ = .088), despite being statistically significant.

**The Signature of Sequence**

The contrast between adjacent and skip-level effects distinguishes a sequential structure from a set of merely correlated behaviours, and we examined it directly through a mediation test. Estimated alone, foundational hygiene exerted a substantial total effect on advanced protection (β = .516, p < .001). When proactive defence was entered alongside it, the direct effect of hygiene attenuated to β = .338 (p < .001), an attenuation of .178, while proactive defence itself carried β = .459 (p < .001). The model accounted for 44.7 per cent of the variance in advanced protection.

Therefore, foundational hygiene substantially reaches advanced protection, though not exclusively, through proactive defence. Its influence is partly transmitted by the intervening stratum rather than exerted directly upon the distant one. Taken with the effect-size pattern- capability transferring strongly between adjacent levels and weakly across them, this constitutes the empirical signature of an ordered structure. A set of parallel behaviours sharing a common disposition would not produce it; such a set would yield comparable associations regardless of the ordinal distance between behaviours.

The structure is nonetheless ordered rather than strictly sequential. The direct path from hygiene to advanced protection, though small, remained significant when the intervening level was controlled, indicating that foundational competence contributes to advanced practice by a route that does not pass through proactive defence. The hierarchy is a graded structure with a retained direct channel, not a strict chain in which each level communicates only with its neighbour.

**Prevalence and Dependency are Distinct**

The descriptive pattern of practice tracks the hierarchy, but only partially. Foundational hygiene was the most widely practised stratum (M = 4.10, SD = 0.72), and advanced protection the least (M = 3.54, SD = 0.75), consistent with a structure that is broad at its base and narrow at its apex. However, proactive defence and recovery recorded identical means (M = 3.70), so the descriptive gradient is not monotonic across the four strata.

This is worth stating plainly rather than eliding, and it carries a conceptual point. Prevalence and dependency are distinct properties. Recovery and help-seeking are reactive behaviours, performed when circumstances demand them rather than maintained as ongoing practice, so their reported frequency reflects the incidence of incidents as much as users' capability. The hierarchy is a claim about what enables what, not about what is done most often. The structural evidence bears on the former; the descriptive means bear on the latter, and only loosely.

**Does the Hierarchy Matter for Outcomes?**

Suppose protective capability is developmental, a question follows: which stratum matters for outcomes? Within the larger study, the four constructs were modelled as predictors of sustained safe continuance, the maintenance of safe participation on social media despite exposure to social engineering. Here, continuance is understood in the self-regulatory sense established in the information-systems literature, in which continued use is conditioned on the ongoing management of the risks and costs of participation rather than on initial adoption alone (Lin et al., 2014).

The result is instructive. Foundational hygiene significantly predicted sustained safe continuance ($\beta = .239$, $p = .022$), whereas advanced protection did not ($\beta = -.117$, $p = .480$). The pattern held under composite estimation (hygiene $\beta = .181$, $p = .006$; advanced protection $\beta = -.040$, $p = .595$).

It is the hierarchy base and not its apex that bears on the outcome. This is not a paradox but a consequence of the structure. Foundational hygiene is routine and continuous, exerting protective influence across the whole of a user's ordinary participation. Advanced protection is occasional and situation-specific; it confers capability without conferring the habitual vigilance on which safe continuance principally rests. The hierarchy explains how capability is built; it does not follow that its highest stratum is the one that most protects.

**Qualitative Corroboration**

The focus-group evidence corroborated the structure from the standpoint of users' own accounts. Participants described a repertoire of protective practice that was explicitly graduated: recognition of the warning signs of deception and habitual caution at its base; strong passwords, two-factor authentication, and configured privacy settings above that; verification of suspicious contacts, blocking, and reporting above that; and, following an incident, credential changes, account securing, and transaction monitoring at its apex.

Two features of these accounts bear on the developmental claim. Participants cumulatively and informally described acquiring these competencies, from experience, peers, and the aftermath of incidents, rather than receiving them as a set through formal instruction. Thus, they described the more demanding

behaviours as things they had come to do, rather than as things they had always done, which is the phenomenology a developmental structure would predict.

Because the discussions were documented as structured thematic records rather than verbatim transcripts, representative participant quotations are not available for reproduction, and none are presented; doing so would misrepresent the evidentiary basis of the strand. The credibility of the qualitative findings therefore rests on two supports other than verbatim illustration. The first is the recurrence of these themes across ten independently constituted groups drawn from two distinct populations differing in age, occupation, and social setting, a consistency unlikely to arise from a single group or moderator. The second, and the stronger, is the convergence of the themes, generated without reference to the structural estimates, with the quantitative findings reported above. This constraint on the qualitative record is stated among the study's limitations.

## Discussion

### Protective Capability is Developmental

The evidence supports the proposition that protective security behaviours are ordered rather than parallel. All four hypothesised paths were supported; the coefficients strengthened monotonically toward the apex of the hierarchy; adjacent-level effects were large while the skip-level effect was small; and the level substantially mediated the influence of the base upon a non-adjacent stratum between them. The four behaviours are not interchangeable manifestations of a single protective disposition. They stand in a structural relation, in which competence at each level furnishes the capability required at the next.

The qualification established in §4.3 should be carried forward: the structure is graded rather than strictly chained. Foundational hygiene retains a direct, if modest, influence on advanced protection alongside its indirect influence. The claim is that protective capability is ordered, not that it is a rigid ladder from which no rungs may be skipped.

### Theoretical Implications

The principal theoretical implication concerns the coping-appraisal component of protection motivation theory. The theory holds that protective action depends on response efficacy and self-efficacy, but it treats these as properties of the individual in relation to a given threat and response. The study findings indicate that self-efficacy for protective action accumulates hierarchically: the confidence to perform demanding protective behaviours is built upon competence acquired through less demanding ones. Therefore, coping appraisal is not a single quantity attaching to a single response, but a stratified capacity that develops. This is an extension of the theory rather than a challenge to it and it is one of the theory's own mechanisms that is implied once followed through.

The findings also speak to the attitude–behaviour gap identified in cyber resilience research, which observes that users holding protective intentions frequently fail to enact them (Goliath et al., 2026). The developmental account supplies a candidate explanation. Suppose advanced protective behaviour presupposes foundational competence; then a user who holds the intention to act protectively but lacks the foundational stratum will be unable to enact the intention, not from insufficient motivation, but from an absent base. The gap between attitude and behaviour may be, in part, a gap in the hierarchy.

Finally, the results qualify the prevailing measurement practice. Where protective behaviours are entered into models as reflective indicators of a single latent construct, the assumption is that they are interchangeable effects of a common cause. The present evidence indicates they are not. A protective composite that averages hygiene with advanced protection averages across strata that stand in a causal relation to one another, and it will obscure precisely the structure that matters.

**Practical Implications**

The practical implication is that security education should be sequenced, not merely comprehensive. A program that delivers advanced countermeasures to users who have not established foundational habits is building upon a base the analysis shows to be a precondition. The design principle that follows is to establish routine hygiene first, strong and distinct authentication, habitual verification, basic privacy configuration, and to introduce proactive, advanced, and recovery-oriented competencies only upon that foundation.

This has a corollary that is encouraging in resource-constrained settings. Because it is the base of the hierarchy that predicts sustained safe participation (§4.5), the most consequential protective competence is also the most accessible one. Interventions aimed at ordinary users need not aspire to technical sophistication; they need to embed consistency. That is a lower bar than the security-education literature often sets, and the evidence suggests it is the bar that matters.

A second corollary concerns how the strata are built. Participants reported acquiring their repertoire informally and cumulatively, and the literature indicates that sustained, repeated training produces more durable behavioural improvement than one-off instruction (Tóth et al., 2025; Alsulami & Dupuis, 2024). A developmental structure and a cumulative acquisition process together imply that security education should be continuous and staged rather than delivered as a single intervention.

**Limitations**

We experienced four limitations during the study. The sample was concentrated among young (91.4% aged 18–24 years), educated, and predominantly female (74.3%) users. Therefore, the hierarchy is established for this population, and its generalisation to older or less educated users is a matter for testing. This bears on the developmental claim in a specific way: an older cohort, whose members acquired digital competence later and under different conditions, might exhibit a different ordering, or a weaker one.

The design was cross-sectional. A developmental structure is a claim about acquisition over time, and the present data establish the structure of relationships among behaviours at a single moment rather than observing their sequence of acquisition. The evidence is consistent with a developmental process and is difficult to explain otherwise, but it does not observe that process. A longitudinal design tracing the acquisition of protective behaviours across waves would test the developmental claim directly, and this is the most important next step for this line of work.

Proactive defence fell marginally below the conventional reliability threshold ($\alpha = .656$), and its AVE fell below .50, so estimates involving that construct carry more measurement error than the others. Since measurement error attenuates observed associations, this works against rather than for the findings involving proactive defence, the mediation it carries is likely understated rather than manufactured.

The qualitative strand was documented as thematic records rather than verbatim transcripts, so it supports the identification of themes and their recurrence across ten independently constituted groups, but not the quotation or attribution of individual participants. Its corroborative role is bound accordingly.

## 5.0 CONCLUSION AND RECOMMENDATIONS

**Conclusion:** Protective cyber security behaviours are not a parallel set of practices that users adopt independently. They are an ordered structure of capability, in which foundational hygiene enables proactive defence, proactive defence enables advanced protection, and advanced protection enables the recovery and help-seeking that presuppose it, with the dependence of each stratum on the one beneath it intensifying as the hierarchy ascends. Capability transfers strongly between adjacent strata and weakly across them, and the influence of the base upon distant strata is substantially transmitted through the levels between. The finding extends protection motivation theory by showing that self-efficacy for protective action accumulates hierarchically rather than attaching to responses singly.

**Recommendations:** The study offers a candidate explanation for the attitude-behaviour gap in cyber resilience, which may in part be a gap in the hierarchy. Ultimately, the study implies that security education must be sequenced rather than merely comprehensive, a conclusion made more tractable, not less, by the further finding that it is the accessible base of the hierarchy, and not its sophisticated apex, that most sustains safe participation.

## 6.0 REFERENCES


1. Alsulami, S., & Dupuis, M. (2024). The effectiveness of education and fear appeal to prevent spear phishing attacks. *2024 Cyber Awareness and Research Symposium (CARS 2024).* https://doi.org/10.1109/CARS61786.2024.10778693
2. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
3. Debb, S. M., & McClellan, M. K. (2021). Perceived vulnerability as a determinant of increased risk for cybersecurity risk behavior. *Cyberpsychology, Behavior, and Social Networking, 24*(9), 605–612. https://doi.org/10.1089/cyber.2021.0043
4. Dzidzah, E., Owusu, K. K., & Asante, B. K. (2020). Security behavior of mobile financial service users. *Information and Computer Security, 28*(5), 719–735. https://doi.org/10.1108/ICS-02-2020-0021
5. Frauenstein, E. D. (2019). An investigation into students' responses to various phishing emails and other phishing-related behaviors. *Communications in Computer and Information Science, 973*, 44–59. https://doi.org/10.1007/978-3-030-11407-7_4
6. Goliath, S., Tsibolane, P., & Snyman, D. (2026). Exploring the cybersecurity–resilience gap: An analysis of student attitudes and behaviors in higher education. *Communications in Computer and Information Science, 2661*, 185–200. https://doi.org/10.1007/978-3-032-09660-9_19
7. Gwenhure, A. K. (2025). University students' security behavior against email phishing attacks: Insights from the health belief model. *Journal of Cybersecurity, 11*(1). https://doi.org/10.1093/cybsec/tyaf034
8. Hasan, M. M., Rahman, K. M., Nath, A., Fuad, M. N., Inthakab, K. S. M., & Emee, A. F. (2025). Understanding user adoption of cybersecurity practices through awareness and perception for enhancing network security in Bangladesh. *2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS 2025).* https://doi.org/10.1109/COMPAS67506.2025.11381666

9. Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security, 24*(3). https://doi.org/10.1007/s10207-025-01032-0
10. Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). Guilford Press.
11. Lin, H., Fan, W., & Chau, P. Y. K. (2014). Determinants of users' continuance of social networking sites: A self-regulation perspective. *Information and Management, 51*(5), 595–603. https://doi.org/10.1016/j.im.2014.03.010
12. Naeem, N.-I.-K., & Mushibwe, C. P. (2025). Navigating digital worlds: A scoping review of skills and strategies for enhancing digital resilience among higher education students on social media platforms. *Discover Education, 4*(1). https://doi.org/10.1007/s44217-025-00432-7
13. Ng, T. H., Lim, Y. Z., & Chan, K. H. (2026). A mobile wallet security: What drives users to protect themselves? *Studies in Big Data, 185*, 403–418. https://doi.org/10.1007/978-3-032-14698-4_38
14. Ngo, F. T., Agarwal, A., & Holman, K. (2026). Cyber hygiene and cyber victimisation among limited English proficiency (LEP) internet users: A mixed-method study. *Victims and Offenders, 21*(5), 969–991. https://doi.org/10.1080/15564886.2024.2329765
15. Risteski, P., Mechkaroska, D., Karamachoski, J., & Duman, S. (2026). The role of human error in cybersecurity threats – Minimising risks in information systems. *Communications in Computer and Information Science, 2669*, 566–578. https://doi.org/10.1007/978-3-032-07373-0_42
16. Saleem, M., Kumar, R., Chawla, C., & Singh, M. (2024). Understanding the human factors in the psychology of cyber threats. In *Human impact on security and privacy: Network and human security, social media, and devices* (pp. 39–58). https://doi.org/10.4018/979-8-3693-9235-5.ch003
17. Sari, P. K., Handayani, P. W., Hidayanto, A. N., & Busro, P. W. (2023). How information security management systems influence the healthcare professionals' security behaviour in a public hospital in Indonesia. *Interdisciplinary Journal of Information, Knowledge, and Management, 18*, 583–602. https://doi.org/10.28945/5185
18. Szczuka, Z., Siwa, M., Abraham, C., Baban, A., Brooks, S., Cipolletta, S., … Luszczynska, A. (2023). Handwashing adherence during the COVID-19 pandemic: A longitudinal study based on protection motivation theory. *Social Science and Medicine, 317*, Article 115569. https://doi.org/10.1016/j.socscimed.2022.115569
19. Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics* (7th ed.). Pearson.
20. Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behaviour towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly, 38*(2), Article 101572. https://doi.org/10.1016/j.giq.2021.101572
21. Tóth, R., Dubniczky, R. A., Limonova, O., & Tihanyi, N. (2025). Sustaining cyber awareness: The long-term impact of continuous phishing training and emotional triggers. *Proceedings of the IEEE International Conference on Big Data*, 7854–7863. https://doi.org/10.48550/arXiv.2510.27298
22. van der Schyff, K., & Flowerday, S. (2021). Mediating effects of information security awareness. *Computers and Security, 106*, Article 102313. https://doi.org/10.1016/j.cose.2021.102313
23. Wright, T., Ruhwanya, Z., & Ophoff, J. (2024). Using the theory of interpersonal behaviour to explain employees' cybercrime preventative behaviour during the pandemic. *Information and Computer Security, 32*(4), 436–452. https://doi.org/10.1108/ICS-11-2023-0228
24. Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). Investigation into phishing risk behaviour among healthcare staff. *Information, 13*(8), Article 392. https://doi.org/10.3390/info13080392