Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Knowing but not doing: A cross-sectional study of how attitude links cyber hygiene knowledge and practice among allied health undergraduates in Nigeria

Adesegun Nurudeen Osijirin

adesegunosijirin@fuahse.edu.ng

Federal University of Allied Health Sciences

Phina Chinelo Ezeagwu

Federal University of Allied Health Sciences

Shamsuddeen Mohammed Sada

Federal University of Allied Health Sciences

Utibe Edmond Victor

Federal University of Allied Health Sciences

Valentine Arinzechukwu Khama

Enugu State University of Science and Technology

John Adeniran Ikuesan

Federal University of Allied Health Sciences

Nsangaette Asuquo Udo

Federal University of Allied Health Sciences

Research Article

Keywords: Computer security, Cyber hygiene, Health knowledge, attitudes, practice, Allied health personnel, Health informatics education, Nigeria

Posted Date: November 17th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11748387/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Knowing but not doing: A cross-sectional study of how attitude links cyber hygiene knowledge and practice among allied health undergraduates in Nigeria

Adesegun Nurudeen Osijirin[a,*], Phina Chinelo Ezeagwu[a], Shamsuddeen Mohammed Sada[b], Utibe Edmond Victor[c], Valentine Arinzechukwu Khama[d], John Adeniran Ikuesan[e], Nsangaette Asuquo Udo[f]

[a] Department of Healthcare Management, Federal University of Allied Health Sciences, Enugu, Nigeria

[b] Department of Software Engineering, Federal University of Allied Health Sciences, Enugu, Nigeria

[c] Department of Health Information Management, Federal University of Allied Health Sciences, Enugu, Nigeria

[d] Department of Mathematics and Computer Science Education, Enugu State University of Science and Technology, Agbani, Enugu, Nigeria

[e] Department of Dental Therapy, Federal University of Allied Health Sciences, Enugu, Nigeria

[f] Department of Artificial Intelligence, Federal University of Allied Health Sciences, Enugu, Nigeria

∗**Corresponding author:** Adesegun Nurudeen Osijirin, Federal University of Allied Health Sciences, P.M.B. 01473, Trans Ekulu, Enugu 400103, Nigeria.

E-mail: adesegunosijirin@fuahse.edu.ng

ORCID: 0009-0002-1053-0913 (Adesegun Nurudeen Osijirin)

0000-0002-3759-6720 (Phina Chinelo Ezeagwu)

0009-0006-0802-1756 (Shamsuddeen Mohammed Sada)

0009-0000-7714-9995 (Utibe Edmond Victor)

0009-0003-0030-7870 (Valentine Arinzechukwu Khama)

0000-0002-9145-6534 (John Adeniran Ikuesan)

0009-0004-9511-5413 (Nsangaette Asuquo Udo)

Acknowledgements: The authors thank the students of the Federal University of Allied Health Sciences, Enugu, who took part in the survey.

Article type: Research. **Journal section:** Education and Training.

Abstract

Background: Allied health professionals increasingly handle electronic health records, connected diagnostic devices and telehealth data, yet the cyber hygiene of allied health students in sub-Saharan Africa is rarely measured.

Objectives: To assess cyber hygiene knowledge, attitudes and practices (KAP) among allied health undergraduates in Nigeria and to test whether attitude mediates the effect of knowledge on practice.

Methods: A cross-sectional survey of 277 undergraduates across six faculties of the Federal University of Allied Health Sciences, Enugu, used a 39-item questionnaire (Kuder–Richardson 20 reliability 0.80–0.85). Predictors of practice were examined with hierarchical linear and logistic regression and bootstrapped mediation analysis, with faculty-weighted and cluster-robust sensitivity analyses.

Results: Mean scores were 61.3% for knowledge, 64.5% for attitude and 43.4% for practice; 62.8% of students had poor practice. Fewer than one in four used unique passwords (24.5%), two-factor authentication (24.5%) or backups (23.5%), and only 30.0% saw themselves as likely targets. Knowledge (standardised $\beta = 0.33$) and attitude ($\beta = 0.38$) explained a further 30.8% of the variance in practice beyond demographic factors (final $R^2 = 0.42$). Attitude carried 35.4% of the effect of knowledge on practice (indirect effect 0.13; 95% confidence interval 0.08–0.18). Formal training was associated with higher scores in all three domains but had no direct effect on practice once knowledge and attitude were controlled.

Conclusions: Future allied health workers know more than they practise. Health informatics curricula should pair hands-on drills in password managers, two-factor authentication and backups with content that raises personal risk perception.

Keywords: Computer security; Cyber hygiene; Health knowledge, attitudes, practice; Allied health personnel; Health informatics education; Nigeria

1 Introduction

Cybercrime has grown rapidly across Africa as internet and mobile-money use have expanded faster than the safeguards around them. Nigeria sits at the centre of this picture: its large, young and highly connected population makes it both a source and a target of fraud, account takeover and social-engineering attacks [1].

The health sector raises the stakes. Healthcare is among the sectors most targeted by cyberattacks, and because medical records hold permanent personal, clinical and genetic details, the harm done to patients by a breach cannot be reversed [2]. Many breaches begin with a human action, such as a reused password or a click on a convincing link [3]. Allied health professionals, including laboratory scientists, radiographers, physiotherapists, dental therapists, health information managers and biomedical engineers, now work daily with electronic health records (EHRs), networked diagnostic devices and telehealth platforms, so their personal security habits become part of the security of the health information system. In Nigeria these habits also carry legal weight: the Nigeria Data Protection Act 2023 sets duties for anyone who processes personal and health data, and the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, amended in 2024, criminalises online fraud and identity theft. The International Medical Informatics Association (IMIA) accordingly lists data protection and information security among the informatics competencies that all health professionals should acquire during their education [4].

Security habits are formed early, and university is where future health workers first meet institutional information systems. Yet research on students' cybersecurity in Nigeria remains uneven. Most studies sample computing or general undergraduate populations, report awareness descriptively, and rarely test how knowledge and attitude translate into behaviour [5]. International studies show that awareness often fails to produce protective action [6,7], and a recent study of nursing students found that most had never received cybersecurity education [8]. To our knowledge, no study has assessed cyber hygiene KAP among students of a specialised allied health university in Nigeria, or modelled the pathway from knowledge through attitude to practice in this group. The present study therefore measures a behavioural outcome (hygiene practice) rather than awareness alone, tests a theory-based pathway from knowledge through attitude to practice, and identifies specific, modifiable gaps that health informatics curricula can target.

1.1 Cyber hygiene as a construct

Cyber hygiene names the routine user behaviours that prevent most security failures: strong and unique passwords, multi-factor authentication, prompt updates, backups, careful handling of links and attachments, and protection of personal data [9,10]. Cain et al. found that even users who rated themselves as knowledgeable

reported poor hygiene, such as password reuse and failure to update [9]. Vishwanath et al. gave the construct a formal definition and an 18-item inventory covering device and storage hygiene, transmission hygiene, social media hygiene, authentication and credential hygiene, and email and messaging hygiene [10]. Parsons et al. showed with the Human Aspects of Information Security Questionnaire (HAIS-Q) that knowledge and attitude each predict self-reported security behaviour [11]. Together these studies justify measuring cyber hygiene as three linked components rather than as general "awareness".

1.2 Evidence from students and health learners

Studies of university students consistently report moderate awareness and weaker practice. In north-eastern Nigeria, Garba et al. surveyed 441 students and found basic knowledge of internet banking risks but only moderate awareness of self-protection [5]. In Saudi Arabia, Alzubaidi reported gaps between general awareness of cybercrime and the protective measures people actually used [12]. Across four countries, Zwilling et al. found that users were aware of threats but applied only minimal protections [7]. Health learners form a distinct group because they will handle confidential patient data. Yalcinkaya et al. surveyed 434 nursing students in Türkiye: 92.9% had never had cybersecurity education, and practice correlated moderately with cybercrime awareness ($r = 0.58$) [8]. Hadlington linked attitudes towards cybersecurity with risky online behaviour [13]. Comparable evidence from Nigerian allied health students is, to our knowledge, absent.

1.3 Theoretical framework and hypotheses

The study uses the knowledge–attitude–practice (KAP) model, supported by protection motivation theory (PMT). The KAP model holds that knowledge shapes attitudes, and that both shape practice [11]. PMT specifies the content of that attitude. People adopt protective behaviour when they perceive a threat as likely (*susceptibility*) and serious (*severity*), and believe that the response works and that they can perform it (*response efficacy* and *self-efficacy*) [14]. The theory of planned behaviour likewise places attitude as the proximal driver of intention and action [15]. Several attitude items in this study map directly onto PMT constructs (Section 3.3). From this framework, three hypotheses were tested:

- **H1:** Knowledge is positively associated with practice.
- **H2:** Attitude is positively associated with practice after controlling for knowledge and demographic characteristics.
- **H3:** Attitude partially mediates the effect of knowledge on practice.

1.4 Objectives

Among undergraduates of the Federal University of Allied Health Sciences (FUAHS), Enugu, the study aimed to measure cyber hygiene KAP, identify the weakest items, compare scores across student characteristics, and test the pathway from knowledge through attitude to practice (H1–H3).

2 Methods

2.1 Design and setting

This was an institution-based cross-sectional survey, reported according to the Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) guidelines [16]; the completed checklist is provided as Online Resource 1. It was conducted at FUAHS, a federal university in South-East Nigeria with six faculties: Basic Medical Sciences; Dental Health; Health Engineering and Technology; Healthcare Management and Leadership; Healthcare Services; and Rehabilitative Health. Data were collected between 10 and 14 August 2026.

2.2 Population, sample size and sampling

The study population comprised the 1,487 registered undergraduate students of FUAHS in the 2025/2026 academic session, according to the university's institutional records. The minimum sample size was estimated with Cochran's formula for a single proportion, $n_0 = z^2p(1 - p)/d^2$, assuming $p = 0.5$, $z = 1.96$ and a margin of error $d = 0.06$, which gave 267 [17]. Applying the finite population correction, $n = n_0/[1 + (n_0 - 1)/N]$, reduced the minimum to 227. To allow for non-response and to retain adequate numbers for comparisons across faculties, 320 questionnaires were distributed. Participants were selected by stratified cluster sampling. The six faculties formed the strata; within each faculty, classes were selected by random draw, and all students present in the selected classes on the day of administration were invited to take part. Undergraduate students aged 18 years or older who were registered in the session were eligible. Of the 320 questionnaires distributed in the selected classes, 277 were returned and analysed (response rate 86.6%). Because classes differed in size and attendance, sampling fractions ranged from 10.9% in Dental Health to 53.3% in Healthcare Services (Table 1).

Table 1 Sampling frame and achieved sample by faculty

Faculty	Population, N	% of total	Sample, n	% of sample	Sampling fraction, %
Dental Health	467	31.4	51	18.4	10.9
Rehabilitative Health	284	19.1	40	14.4	14.1
Healthcare Management and Leadership	247	16.6	46	16.6	18.6

Faculty	Population, N	% of total	Sample, n	% of sample	Sampling fraction, %
Basic Medical Sciences	213	14.3	40	14.4	18.8
Health Engineering and Technology	156	10.5	36	13.0	23.1
Healthcare Services	120	8.1	64	23.1	53.3
Total	**1,487**	**100.0**	**277**	**100.0**	**18.6**

Faculty sizes from institutional records, 2025/2026 session. Population = registered undergraduates; sampling fraction = sample ÷ population.

2.3 Instrument

A structured, self-administered questionnaire was developed from the cyber hygiene literature [9–11] and adapted to the Nigerian context, including items on the Bank Verification Number (BVN), SIM-swap fraud, the Nigeria Data Protection Act 2023 and Nigerian cybercrime law. It had four sections:

1. **Background (11 items):** gender, age, level of study, faculty, prior formal cybersecurity training, average daily internet use, cyber incident in the past 12 months, and first source of cybersecurity information.
2. **Knowledge (19 scored items):** three multiple-choice items (phishing, password strength and two-factor authentication) and 16 true/false/not-sure statements. Correct answers scored 1; incorrect, "not sure" and "I don't know" responses scored 0 (range 0–19).
3. **Attitude (10 items):** seven five-point Likert items and three yes/no/not-sure items. Favourable responses (agree or strongly agree; "yes"; disagreement with the reverse-worded password-sharing item) scored 1 (range 0–10).
4. **Practice (10 items):** frequency of ten hygiene behaviours on a five-point scale from never to always; "often" or "always" scored 1 (range 0–10).

Two cybersecurity experts and one health-education specialist reviewed content validity, and the instrument was pre-tested on 20 students outside the sample. Internal consistency was assessed with the Kuder–Richardson Formula 20 (KR-20) for the dichotomously scored scales and was good for knowledge (0.80), attitude (0.82) and practice (0.85); Cronbach's α for the practice items on their original five-point scale was 0.93. Values of 0.70 or above were taken as acceptable [18].

2.4 Classification of KAP levels

Each score was converted to a percentage of its maximum and classified with Bloom's cut-offs, which are widely used in KAP research: good (≥ 80%), moderate (60–79%) and poor (< 60%). For attitude, these levels are reported as positive, neutral and negative. For the logistic model, *adequate practice* was defined as a practice score of 6 or more (≥ 60%).

2.5 Statistical analysis

Data were entered into an Excel workbook with drop-down lists that blocked out-of-range entries and analysed in Python 3 (pandas, NumPy and SciPy). Sixteen questionnaires (5.8%) had one unanswered item; in line with the pre-specified scoring rule, an unanswered item was scored 0 and all 277 cases were retained. Descriptive statistics are reported as frequencies, percentages, means, standard deviations, medians and interquartile ranges (IQR).

Because all three scores departed from normality (Shapiro–Wilk $p < 0.001$), bivariate analyses used the Mann–Whitney U test for two groups, the Kruskal–Wallis H test for three or more groups, and Spearman's ρ for correlations among knowledge, attitude and practice.

Predictors of practice were examined with three-step hierarchical linear regression. Model 1 entered gender, age ($\geq$ 24 years), level of study (300 level or above), prior training, daily internet use ($\geq$ 5 h), cyber-incident experience and faculty (reference: Basic Medical Sciences); Model 2 added knowledge; and Model 3 added attitude. Multicollinearity was checked with variance inflation factors (VIF). A binary logistic regression with the same predictors modelled adequate practice. Mediation of the knowledge–practice effect by attitude was tested with the product-of-coefficients method, adjusting for all covariates, with a percentile 95% confidence interval (CI) from 5,000 bootstrap resamples [19]. Statistical significance was set at $p < 0.05$ (two-tailed).

Two sensitivity analyses addressed the sampling design. First, because the faculty distribution of the sample differed from that of the population, the main descriptive estimates, the final regression model and the mediation analysis were re-estimated with post-stratification weights equal to each faculty's population share divided by its sample share. Second, because whole classes were sampled, the final regression model was re-estimated with cluster-robust standard errors, treating each faculty-by-level group as a cluster (30 clusters), and the intraclass correlation of the practice score was used to estimate the design effect.

2.6 Ethical considerations

Ethical approval was obtained from the Research Ethics Committee of the Faculty of Healthcare Management and Leadership, Federal University of Allied Health Sciences, Enugu (approval no. RE/FHCML/VOL.1/01/XII, dated 7 June 2026). Participation was voluntary and anonymous. Respondents gave informed consent before completing the questionnaire, no personal identifiers were collected, and the data were stored on password-protected devices in line with the Nigeria Data Protection Act 2023.

2.7 Use of artificial intelligence tools

The study was designed, conducted and interpreted by the authors, who also wrote the manuscript. Claude (Anthropic; model Claude Opus 5.5), accessed through the claude.ai web interface with default settings in November 2026, was used to generate Python code for statistical analyses specified or approved by the authors. Inputs were the anonymised dataset and the authors' analysis plan; representative prompts are available from the corresponding author. The authors re-checked all statistical outputs against the dataset and take full responsibility for the content.

3 Results

3.1 Characteristics of respondents

All 277 respondents were undergraduates. Just over half were female (54.5%), and most were aged 18–23 years (76.5%) and in 100–400 level (95.3%). Healthcare Services contributed the largest share (23.1%), reflecting its high sampling fraction (Table 1). Only 48 students (17.3%) had ever received formal cybersecurity training; 23.5% reported a cyber incident in the past year and a further 18.1% were unsure. Social media was the most common first source of cybersecurity information (39.4%), whereas formal lectures accounted for 19.5% (Table 2).

Table 2 Characteristics of respondents (N = 277)

Characteristic	Category	n	%
Gender	Female	151	54.5
	Male	126	45.5
Age (years)	18–20	98	35.4
	21–23	114	41.2
	24–26	52	18.8
	≥27	13	4.7
Level of study	100 level	71	25.6
	200 level	68	24.5
	300 level	65	23.5
	400 level	60	21.7
	500 level	13	4.7
Faculty	Healthcare Services	64	23.1
	Dental Health	51	18.4
	Healthcare Management and Leadership	46	16.6
	Basic Medical Sciences	40	14.4
	Rehabilitative Health	40	14.4
	Health Engineering and Technology	36	13.0
Formal cybersecurity training	Yes	48	17.3

Characteristic	Category	n	%
	No	229	82.7
Daily internet use	< 2 h	23	8.3
	2–4 h	86	31.0
	5–8 h	110	39.7
	> 8 h	58	20.9
Cyber incident, past 12 months	Yes	65	23.5
	No	162	58.5
	Not sure	50	18.1
First source of cybersecurity information	Social media	109	39.4
	Lecture/course	54	19.5
	News media	42	15.2
	Workshop/training	38	13.7
	Family/friends	28	10.1
	Never heard of it	6	2.2

Percentages may not sum to 100 because of rounding.

3.2 Overall KAP levels

Practice lagged well behind knowledge and attitude. Mean practice was 43.4% of the maximum, compared with 61.3% for knowledge and 64.5% for attitude. Nearly two in three students (62.8%) had poor practice, and fewer than one in five had good knowledge (18.8%) or good practice (17.3%). Attitude was the strongest component, with 43.0% of students positive (Table 3).

Table 3 Knowledge, attitude and practice scores and levels (N = 277)

Domain	Range	Mean ± SD	Median (IQR)	% of max.	Good/positive, n (%)	Moderate/neutral, n (%)	Poor/negative, n (%)
Knowledge	0–19	11.64 ± 4.14	12 (8–15)	61.3	52 (18.8)	100 (36.1)	125 (45.1)
Attitude	0–10	6.45 ± 2.79	7 (4–9)	64.5	119 (43.0)	74 (26.7)	84 (30.3)
Practice	0–10	4.34 ± 2.95	4 (2–7)	43.4	48 (17.3)	55 (19.9)	174 (62.8)

Levels by Bloom's cut-offs: good ≥ 80%, moderate 60–79%, poor < 60% of the maximum score. KR-20: knowledge 0.80, attitude 0.82, practice 0.85. IQR, interquartile range; SD, standard deviation.

3.3 Item-level knowledge, attitude and practice

Knowledge. Students recognised familiar threats but misread the limits of common safeguards (Fig. 1). Most knew that online fraud is a crime (80.5%), what phishing is (79.4%) and that an unrequested one-time password (OTP) signals an intrusion attempt (75.8%). Only a third knew that the HTTPS padlock does not prove a website is legitimate (33.2%). Fewer than half understood SIM-swap fraud (42.2%), file deletion (43.0%), their data protection rights (45.5%), the danger of reusing a strong password (48.7%) or the risk of links from known senders (49.8%).

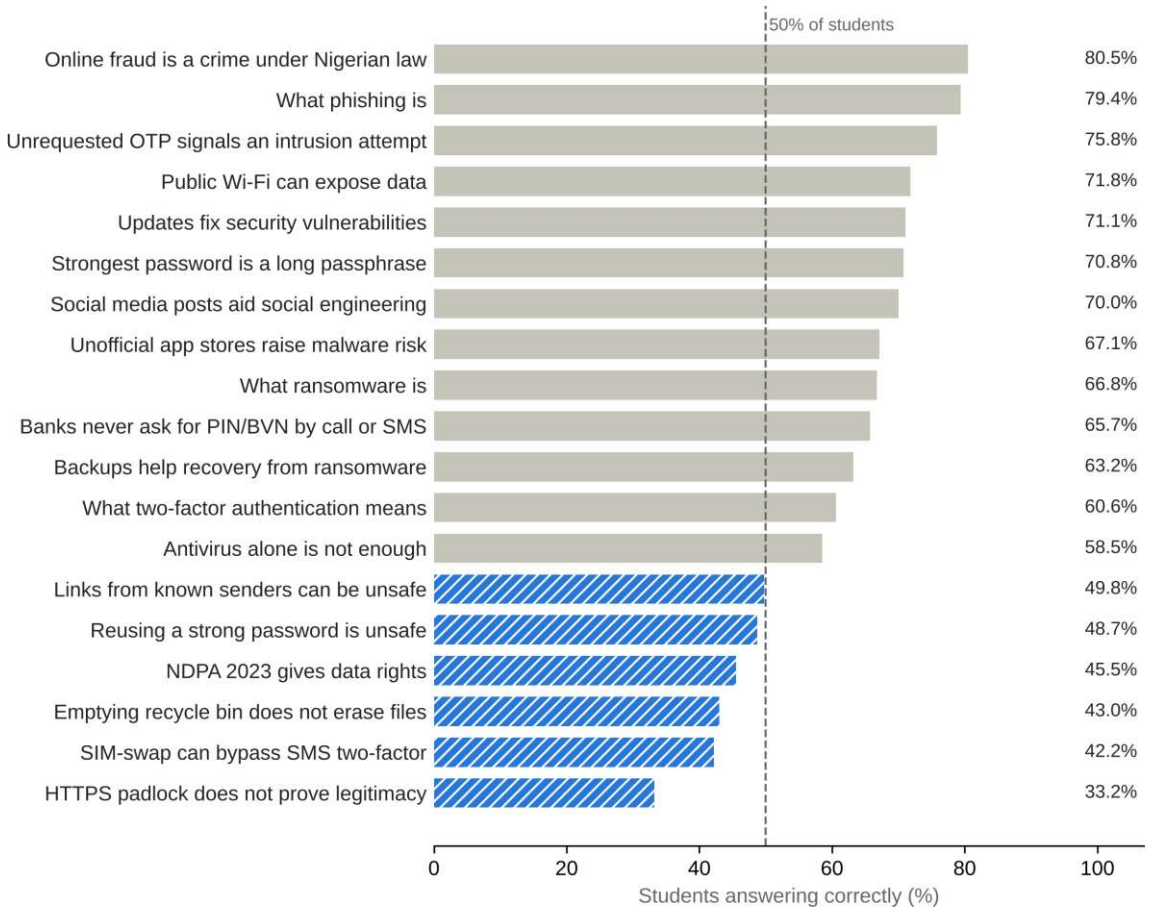


Fig. 1 Percentage of students answering each knowledge item correctly (N = 277). Blue bars mark the six items answered correctly by fewer than half of the students; the dashed line marks 50%

Attitude. Students valued security but did not feel personally at risk (Table 4). Large majorities agreed that good practices are worth the effort (78.7%), wanted to learn more (78.7%) and supported compulsory training (74.7%). Yet only 30.0% saw themselves as likely targets, and just over half felt confident recognising phishing (53.4%) or regarded cracked software as risky (53.4%).

Table 4 Favourable responses to attitude items (N = 277)

Item	Statement	PMT construct	Favourable, %
a4	Good security practices are worth the extra time and effort	Response efficacy	78.7
a9	I am interested in learning more about cybersecurity	–	78.7
a5	Cybersecurity training should be compulsory for all students	–	74.7
a8	Sharing passwords with close friends or partners is acceptable (disagree)	–	72.2
a1	Cybersecurity is my personal responsibility, not only the ICT unit's	Responsibility	71.5
a3	Falling victim would have serious consequences for me	Perceived severity	71.1
a6	I would report a cyber incident to the authorities	–	61.0
a7	I am confident I can recognise a phishing message	Self-efficacy	53.4
a10	Using pirated or cracked software is risky	–	53.4
a2	I am a likely target of cyberattacks	Perceived susceptibility	30.0

Items ordered by percentage favourable. PMT, protection motivation theory; –, no direct PMT mapping.

Practice. Only two behaviours were practised often or always by most students: keeping OTP, PIN and BVN private (79.4%) and locking devices (73.3%) (Fig. 2). Fewer than one in four reviewed app permissions (22.4%), backed up files (23.5%), used different passwords for important accounts (24.5%) or enabled two-factor authentication (24.5%). Knowledge did not carry over into action: 60.6% could define two-factor authentication but only 24.5% used it, and 71.1% knew that updates fix vulnerabilities but only 44.0% installed them promptly.

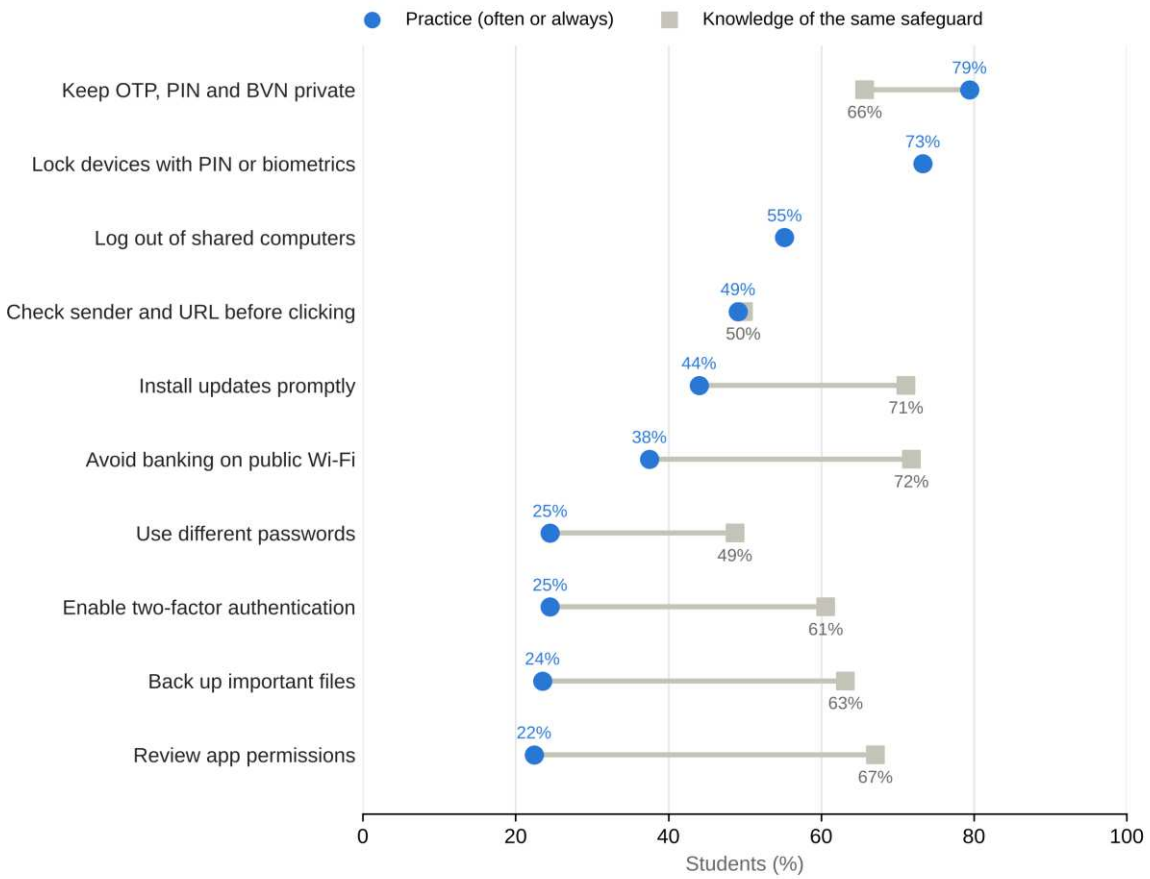


Fig. 2 Practice of each cyber hygiene behaviour (often or always; blue) compared with correct knowledge of the same safeguard (grey) (N = 277). Matching knowledge items: p9–k10, p4–k20, p3–k8, p7–k7, p1–k9, p2–k4, p6–k16, p8–k12; device locking (p5) and logging out of shared computers (p10) had no matching knowledge item

3.4 Differences across groups

Prior training, level of study and faculty were associated with all three scores (Table 5). Trained students scored higher in every domain (all $p < 0.001$). Scores rose with level of study (knowledge $p < 0.001$, attitude $p = 0.008$, practice $p = 0.032$); knowledge, for example, rose from 9.82 in 100 level to 13.85 in 500 level. Health Engineering and Technology students had the highest scores in every domain, and Healthcare Services and

Rehabilitative Health students the lowest practice. Knowledge also rose with age (p = 0.009). Gender, daily internet use and past cyber incidents showed no significant differences.

Table 5 Knowledge, attitude and practice scores by respondent characteristics (mean ± SD)

Variable	Group (n)	Knowledge	Attitude	Practice
Gender	Female (151)	11.42 ± 4.19	6.33 ± 2.86	4.34 ± 2.96
	Male (126)	11.90 ± 4.07	6.59 ± 2.72	4.33 ± 2.96
	p (U test)	0.396	0.483	0.973
Age (years)	18–20 (98)	10.53 ± 4.24	6.09 ± 2.86	4.07 ± 2.93
	21–23 (114)	12.01 ± 3.95	6.50 ± 2.64	4.21 ± 2.96
	24–26 (52)	12.65 ± 4.06	6.65 ± 3.07	4.63 ± 2.93
	≥27 (13)	12.69 ± 3.82	7.85 ± 2.08	6.23 ± 2.68
	p (H test)	**0.009**	0.120	0.077
Level of study	100 (71)	9.82 ± 4.30	5.65 ± 2.86	3.55 ± 2.86
	200 (68)	11.74 ± 4.26	6.21 ± 3.01	4.54 ± 2.93
	300 (65)	11.97 ± 3.82	6.83 ± 2.53	4.34 ± 3.12
	400 (60)	12.85 ± 3.48	6.90 ± 2.66	4.68 ± 2.85
	500 (13)	13.85 ± 3.74	8.08 ± 1.89	5.92 ± 2.36
	p (H test)	**< 0.001**	**0.008**	**0.032**
Faculty	Basic Medical Sciences (40)	11.72 ± 4.13	6.45 ± 2.64	4.38 ± 2.90
	Dental Health (51)	11.10 ± 4.37	6.33 ± 2.65	4.55 ± 2.59
	Health Engineering and Technology (36)	13.94 ± 3.50	7.92 ± 2.20	5.94 ± 3.03
	Healthcare Management and Leadership (46)	12.50 ± 3.72	6.04 ± 3.08	4.20 ± 2.96
	Healthcare Services (64)	10.70 ± 4.18	5.95 ± 2.95	3.67 ± 2.75
	Rehabilitative Health (40)	10.68 ± 3.98	6.52 ± 2.70	3.80 ± 3.25
	p (H test)	**0.001**	**0.018**	**0.011**
Formal training	Yes (48)	13.67 ± 3.62	8.19 ± 1.54	5.77 ± 2.81
	No (229)	11.21 ± 4.12	6.08 ± 2.86	4.03 ± 2.90
	p (U test)	**< 0.001**	**< 0.001**	**< 0.001**
Daily internet use	< 2 h (23)	11.83 ± 3.42	6.91 ± 2.56	3.74 ± 2.85
	2–4 h (86)	10.72 ± 4.39	6.17 ± 3.07	4.14 ± 2.96
	5–8 h (110)	12.05 ± 4.09	6.65 ± 2.61	4.65 ± 2.88
	> 8 h (58)	12.14 ± 3.97	6.29 ± 2.82	4.28 ± 3.12
	p (H test)	0.186	0.734	0.440
Cyber incident, past 12 months	Yes (65)	11.69 ± 4.12	6.86 ± 2.66	4.09 ± 2.96
	No (162)	11.60 ± 4.09	6.37 ± 2.84	4.51 ± 2.95
	Not sure (50)	11.70 ± 4.40	6.16 ± 2.82	4.10 ± 2.96
	p (H test)	0.986	0.353	0.511

Bold p-values are significant at p < 0.05. U, Mann–Whitney U test; H, Kruskal–Wallis H test; SD, standard deviation. Score ranges: knowledge 0–19; attitude and practice 0–10.

3.5 Relationships among knowledge, attitude and practice

The three components were moderately and positively correlated: knowledge–attitude ρ = 0.53, knowledge–practice ρ = 0.54 and attitude–practice ρ = 0.56 (all p < 0.001).

In the hierarchical regression (Table 6), demographic and exposure variables alone explained 10.8% of the variance in practice, with training the only significant predictor (β = 0.19, p = 0.003). Adding knowledge raised R^2 to 0.32 ($\Delta R^2 = 0.22$, $p < 0.001$), and adding attitude raised it to 0.42 ($\Delta R^2 = 0.09$, $p < 0.001$). In the final model both knowledge (β = 0.33) and attitude (β = 0.38) predicted practice, supporting H1 and H2, whereas the effect of training was no longer significant (β = 0.02, p = 0.659). All VIFs were below 2.1.

Table 6 Hierarchical linear regression predicting cyber hygiene practice (N = 277)

Predictor	Model 1 β	Model 2 β	Model 3 B (95% CI)	Model 3 β	Model 3 p
Female (vs male)	−0.01	0.03	0.25 (−0.31, 0.81)	0.04	0.371
Age ≥ 24 years	0.08	0.06	0.35 (−0.36, 1.07)	0.05	0.329
Level ≥ 300	0.08	−0.02	−0.30 (−0.91, 0.31)	−0.05	0.338
Formal training	**0.19**	0.09	0.18 (−0.61, 0.97)	0.02	0.659
Internet use ≥ 5 h/day	0.05	0.00	0.07 (−0.50, 0.64)	0.01	0.810
Incident: yes (vs no)	−0.05	−0.06	−0.58 (−1.27, 0.11)	−0.08	0.099
Incident: not sure (vs no)	−0.08	−0.07	−0.38 (−1.13, 0.37)	−0.05	0.325
Faculty (5 dummies; ref. Basic Medical Sciences)	ns	ns	–	–	all > 0.47
Knowledge score	–	**0.51**	0.23 (0.15, 0.32)	**0.33**	< 0.001
Attitude score	–	–	0.40 (0.28, 0.52)	**0.38**	< 0.001
R^2	0.108	0.323	–	0.417	–
Adjusted R^2	0.068	0.290	–	0.386	–
ΔR^2	–	0.215	–	0.093	–
F (df)	2.67 (12, 264)	9.67 (13, 263)	–	13.37 (14, 262)	–

β, standardised coefficient; B, unstandardised coefficient; CI, confidence interval; ns, not significant. Bold β significant at $p < 0.05$. Model 1 p = 0.002; Models 2 and 3 $p < 0.001$. All variance inflation factors < 2.1.

The logistic model gave the same picture. Each additional knowledge point raised the odds of adequate practice by 26% (OR = 1.26, 95% CI 1.15–1.39), and each additional attitude point by 37% (OR = 1.37, 95% CI 1.18–1.59); no demographic variable was significant (McFadden $R^2 = 0.26$; likelihood-ratio $\chi^2 = 96.4$, $p < 0.001$). In total, 103 students (37.2%) had adequate practice.

Attitude partially mediated the effect of knowledge on practice, supporting H3 (Fig. 3). Knowledge predicted attitude (B = 0.32, $p < 0.001$), and its total effect on practice (B = 0.36) split into a direct effect of 0.23 and an indirect effect through attitude of 0.13 (95% bootstrap CI 0.08–0.18), so attitude carried 35.4% of the total effect. Training predicted both knowledge (β = 0.20, p = 0.001) and attitude (β = 0.17, p = 0.002), which explains why its direct effect on practice disappeared once both were controlled.

The sensitivity analyses did not change these conclusions. With faculty weights, mean scores were 61.1% for knowledge, 64.7% for attitude and 44.0% for practice, and 63.0% of students had poor practice. In the weighted final model, knowledge (β = 0.36) and attitude (β = 0.35) remained the main predictors, training remained non-significant (p = 0.772), and attitude carried 32.3% of the effect of knowledge on practice. With cluster-robust standard errors, knowledge and attitude remained significant (both $p < 0.001$) and training did not (p = 0.676).

The intraclass correlation of practice within faculty-by-level groups was 0.073, giving an estimated design effect of 1.60.

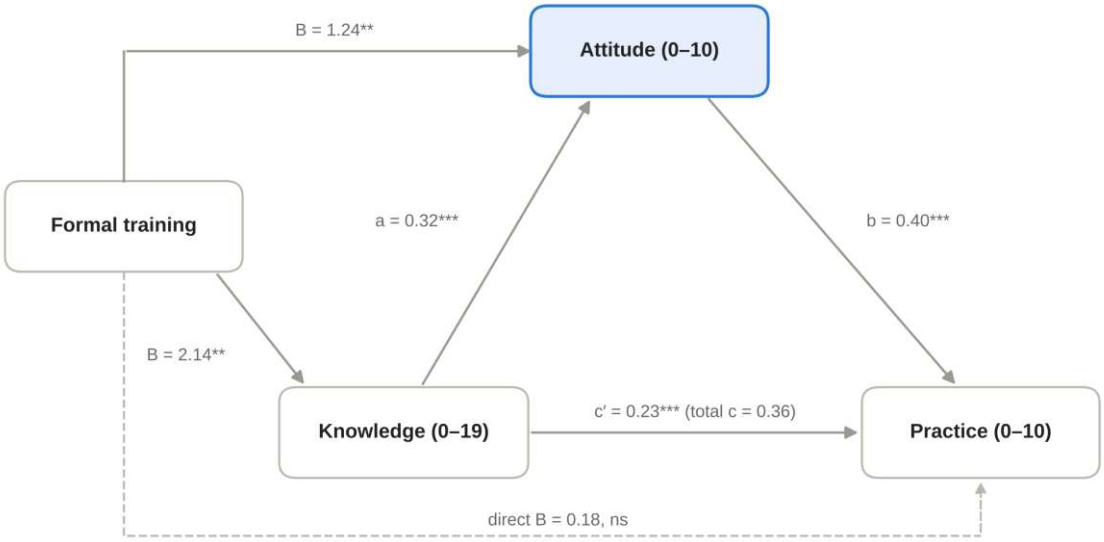


Fig. 3 Path model of knowledge, attitude and practice, including formal training. Unstandardised coefficients (B) adjusted for all covariates (N = 277). Indirect effect a × b = 0.13 (95% bootstrap CI 0.08–0.18), 35.4% of the total effect. ∗∗ $p < 0.01$; ∗∗∗ $p < 0.001$; ns, not significant

4 Discussion

This study found a clear knowledge–practice gap among allied health undergraduates in Enugu. Students had moderate knowledge and a moderately positive attitude, but nearly two-thirds had poor practice. Knowledge and attitude accounted for about three-quarters of the explained variance in practice, and attitude carried about a third of the effect of knowledge. Formal training made a difference, but almost entirely by raising knowledge and attitude. This matters for health informatics because these students will soon hold credentials to EHRs, laboratory systems and imaging archives, where one compromised account can expose many patients.

4.1 Moderate knowledge with specific blind spots

A mean knowledge score of 61% is consistent with the moderate awareness reported among Nigerian students by Garba et al. [5]. The item profile matters more than the mean. Students knew widely publicised threats such as phishing and OTP fraud but misunderstood how safeguards fail. Two in three believed that the HTTPS padlock proves a site is legitimate, a misconception that attackers exploit because phishing sites now routinely carry valid certificates. Fewer than half understood SIM-swap fraud, which undermines the SMS-based two-

factor authentication on which Nigerian banks and many health portals still depend. Fewer than half knew their rights under the Nigeria Data Protection Act 2023, a concern for future health workers who will process sensitive patient data under that law.

4.2 A positive but self-exempting attitude

Students strongly endorsed security in principle: about four in five thought it worth the effort and wanted to learn more. Yet only 30% saw themselves as likely targets. In PMT terms, perceived severity was high but perceived susceptibility was low [14]. Students who believe attacks happen to others have little reason to adopt effortful habits. Confidence in recognising phishing was also modest (53%), pointing to weak self-efficacy. The 61% who were willing to report incidents suggests that reporting channels are either unknown or not trusted.

4.3 Easy habits adopted, effortful ones neglected

The two behaviours most students practised, keeping OTP, PIN and BVN private and locking devices, are simple, visible and heavily promoted by Nigerian banks and phone makers. The neglected behaviours, namely unique passwords, two-factor authentication, backups and permission checks, require setup effort and offer no immediate reward. This mirrors findings that users adopt minimal protections [7] and that knowledge often fails to change behaviour [6,9]. The gap between knowing and doing was sharpest for two-factor authentication (60.6% knew it, 24.5% used it) and updates (71.1% vs 44.0%). These are the same controls that health organisations rely on to protect clinical systems [3], so the gap is likely to follow students into clinical placements unless it is addressed during training.

4.4 What drives practice

Knowledge and attitude were the only significant predictors of practice once both were entered, in line with the KAP model and with HAIS-Q findings that knowledge and attitude jointly shape behaviour [11]. Attitude had a slightly larger standardised effect than knowledge, and it transmitted about 35% of the knowledge effect. Information therefore works best when it changes how students judge their own risk, not only what they know.

Training raised all three scores, but its direct effect on practice disappeared once knowledge and attitude were controlled, so training appears to work through the KAP pathway rather than around it. This differs from Yalcinkaya et al., who found no association between prior cybersecurity education and nursing students' practice scores [8]; the difference may reflect the content and depth of training. With only 17% trained and social media the commonest first source of information, most students' security learning is left to chance.

The absence of gender differences agrees with Zwilling et al. [7]. The higher scores in Health Engineering and Technology are plausible given that faculty's technical curriculum, and the lower practice in Healthcare Services and Rehabilitative Health shows where intervention is most needed. Faculty differences were not significant in the adjusted model, suggesting that they reflect differences in knowledge and attitude rather than discipline itself. Scores also rose with level of study, but practice remained below 50% of the maximum at every level up to 400 level, so progressing through the degree made students better informed faster than it made them safer. Neither internet use nor past incidents was associated with practice: more time online did not build better habits, and victimisation did not appear to prompt behaviour change, a missed teachable moment.

4.5 Implications for health informatics education and practice

The findings point to four actions for FUAHS and similar health sciences institutions, consistent with the IMIA recommendation that information security be part of the informatics preparation of every health professional [4].

1. **Make cyber hygiene a credit-bearing part of the general studies or health informatics curriculum**, starting in 100 level, where scores were lowest.
2. **Teach by doing.** Short sessions in which students install a password manager, switch on app-based two-factor authentication and set up automatic backups target the three most neglected behaviours.
3. **Build perceived susceptibility and self-efficacy** through simulated phishing, local cases of account takeover and SIM-swap losses, and feedback on personal exposure.
4. **Correct the misconceptions identified here** (the HTTPS padlock, SIM-swap risk, password reuse and data protection rights), link them to patient-data responsibilities during clinical placements, and publicise a clear incident-reporting channel.

4.6 Strengths and limitations

Strengths include coverage of all six faculties, random selection of classes, a context-adapted reliable instrument, and a theory-driven mediation analysis rather than descriptive reporting of awareness.

It also has limitations. First, its cross-sectional design shows association, not causation, and the mediation result should be read as consistent with, not proof of, a causal pathway. Second, practice was self-reported and may be inflated by social desirability. Third, data came from undergraduates at one federal university in South-East Nigeria, so the results may not generalise to postgraduate students, to state or private institutions or to other regions. Fourth, small subgroups ($\geq$ 27 years, 500 level) limit comparisons involving them, and pairwise post hoc comparisons were not performed after significant Kruskal–Wallis tests. Fifth, because whole classes were

sampled and attendance varied, the faculty distribution of the sample differed from that of the population, and the sample-size calculation did not include a design effect; allowing for the estimated design effect of 1.60 would have raised the minimum sample to about 363. The sensitivity analyses left the conclusions unchanged, but precision is lower than the nominal confidence intervals suggest. Sixth, scoring unanswered items as 0 may have slightly underestimated the scores of the 16 respondents (5.8%) concerned. Finally, the training item did not capture the type, length or recency of training.

Future studies should include postgraduate students, compare allied health students across several Nigerian universities, measure hygiene behaviours through simulated phishing or device audits, and evaluate a PMT-based training intervention with a controlled pre–post design.

5 Conclusion

Allied health undergraduates at FUAHS, Enugu, know a fair amount about cyber threats and value security, but most do not practise the habits that protect them. Effortful protections such as unique passwords, two-factor authentication and backups are rare, and few students see themselves as targets. Knowledge and attitude together drive practice, and training helps by raising both. Because these students will soon handle patient data in digital health systems, structured, practical cyber hygiene education that also builds personal risk perception should become part of their professional preparation.

Statements and Declarations

Competing interests

The authors have no relevant financial or non-financial interests to disclose.

Funding

No funding was received for conducting this study.

Ethics approval

This study was performed in line with the principles of the Declaration of Helsinki. Approval was granted by the Research Ethics Committee of the Faculty of Healthcare Management and Leadership, Federal University of Allied Health Sciences, Enugu (No. RE/FHCML/VOL.1/01/XII; 7 June 2026).

Consent to participate

Informed consent was obtained from all individual participants included in the study.

Consent to publish

Not applicable. The article contains no data that could identify an individual participant.

Data availability

The anonymised dataset generated and analysed during the current study is available from the corresponding author on reasonable request.

Code availability

The questionnaire and the Python analysis scripts used in this study are available from the corresponding author on reasonable request.

Author contributions

Adesegun Nurudeen Osijirin: Conceptualization, Methodology, Software, Formal analysis, Visualization, Project administration, Writing – original draft, Writing – review & editing. **Phina Chinelo Ezeagwu:** Investigation, Resources, Validation, Writing – review & editing. **Shamsuddeen Mohammed Sada:** Methodology, Supervision, Validation, Writing – review & editing. **Utibe Edmond Victor:** Investigation, Data curation, Writing – review & editing. **Valentine Arinzechukwu Khama:** Methodology, Validation, Writing – review & editing. **John Adeniran Ikuesan:** Investigation, Resources, Writing – review & editing. **Nsangaette Asuquo Udo:** Supervision, Validation, Writing – review & editing. All authors read and approved the final manuscript.

Use of artificial intelligence

Use of an AI tool for data analysis and drafting is reported in Section 2.7.

References

1. Kshetri N (2019) Cybercrime and cybersecurity in Africa. J Glob Inf Technol Manag 22:77–81. https://doi.org/10.1080/1097198X.2019.1603527
2. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin M-V, Calcavecchia F, Anderson D, Burleson W, Vogel J-M, O'Leary C, Eshaya-Chauvin B, Flahault A (2020) Cybersecurity of hospitals: discussing the

challenges and working towards mitigating the risks. BMC Med Inform Decis Mak 20:146. https://doi.org/10.1186/s12911-020-01161-7

3. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S (2021) Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors 21:5119. https://doi.org/10.3390/s21155119

4. Bichel-Findlay J, Koch S, Mantas J et al (2023) Recommendations of the International Medical Informatics Association (IMIA) on education in biomedical and health informatics: second revision. Int J Med Inform 170:104908. https://doi.org/10.1016/j.ijmedinf.2022.104908

5. Garba AA, Siraj MM, Othman SH (2022) An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. Int J Electr Comput Eng 12:572–584. https://doi.org/10.11591/ijece.v12i1.pp572-584

6. Bada M, Sasse AM, Nurse JRC (2019) Cyber security awareness campaigns: why do they fail to change behaviour? arXiv:1901.02672. https://doi.org/10.48550/arXiv.1901.02672

7. Zwilling M, Klien G, Lesjak D, Wiechetek Ł, Cetin F, Basim HN (2022) Cyber security awareness, knowledge and behavior: a comparative study. J Comput Inf Syst 62:82–97. https://doi.org/10.1080/08874417.2020.1712269

8. Yalcinkaya T, Tuncer M, Tuncer GZ, Erol A, Cinar Yucel S (2025) Nursing students' cybersecurity practices and perceptions and cybersecurity crime awareness: a cross-sectional study. Nurse Educ Today 153:106818. https://doi.org/10.1016/j.nedt.2025.106818

9. Cain AA, Edwards ME, Still JD (2018) An exploratory study of cyber hygiene behaviors and knowledge. J Inf Secur Appl 42:36–45. https://doi.org/10.1016/j.jisa.2018.08.002

10. Vishwanath A, Neo LS, Goh P, Lee S, Khader M, Ong G, Chin J (2020) Cyber hygiene: the concept, its measure, and its initial tests. Decis Support Syst 128:113160. https://doi.org/10.1016/j.dss.2019.113160

11. Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C (2014) Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur 42:165–176. https://doi.org/10.1016/j.cose.2013.12.003

12. Alzubaidi A (2021) Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon 7:e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

13. Hadlington L (2017) Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon 3:e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
14. Rogers RW (1975) A protection motivation theory of fear appeals and attitude change. J Psychol 91:93–114. https://doi.org/10.1080/00223980.1975.9915803
15. Ajzen I (1991) The theory of planned behavior. Organ Behav Hum Decis Process 50:179–211. https://doi.org/10.1016/0749-5978(91)90020-T
16. von Elm E, Altman DG, Egger M, Pocock SJ, Gøtzsche PC, Vandenbroucke JP (2007) The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) statement: guidelines for reporting observational studies. Lancet 370:1453–1457. https://doi.org/10.1016/S0140-6736(07)61602-X
17. Cochran WG (1977) Sampling techniques, 3rd edn. Wiley, New York
18. Tavakol M, Dennick R (2011) Making sense of Cronbach's alpha. Int J Med Educ 2:53–55. https://doi.org/10.5116/ijme.4dfb.8dfd
19. Preacher KJ, Hayes AF (2008) Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. Behav Res Methods 40:879–891. https://doi.org/10.3758/BRM.40.3.879

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- CyberHygieneKAPFUAHSUpdated.xlsx