JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Building Cybersecurity Awareness among Teacher Trainees in Nigerian Colleges of Education: Design and Evaluation Protocol for an Eight-Week Module

Abubakar Balarabe Isa[1], Nafiu Abubakar[2], Farouk Umar Yarima[3], Ismail Isah Balarabe[4]

[1&4]*Department of Computer Science, School of Science Education, Sa'adatu Rimi College of Education, Kumbotso, Kano State, Nigeria*

Corresponding author E-mail: balarabesadeeq@gmail.com

ABSTRACT

Colleges of Education play a critical role in preparing future teachers who influence learners' digital practices. However, context-specific approaches to strengthening cybersecurity awareness among pre-service teachers in Nigeria remain limited. This paper proposes an eight-week cybersecurity awareness module integrated into Computer Literacy and Information and Communication Technology (ICT) courses, alongside a protocol for evaluating its effectiveness through a pilot survey. The module is theoretically underpinned by Protection Motivation Theory, the Theory of Planned Behaviour, the Technology Acceptance Model and Self-Efficacy Theory, with particular consideration of resource-constrained educational settings. Its evaluation adopts a quasi-experimental pretest–posttest design involving an intervention group and a comparison group. Outcomes will be assessed through measures of cybersecurity knowledge, attitudes and self-reported practices using an adapted Human Aspects of Information Security Questionnaire (HAIS-Q), phishing-recognition tasks and a delayed follow-up assessment. Four testable hypotheses are formulated based on propositions established in a companion conceptual review. As a design and research protocol paper, this study presents no empirical findings but provides a practical and theoretically informed framework for implementation, evaluation and refinement by teacher educators and cybersecurity researchers in Nigerian Colleges of Education.

Keywords: Cybersecurity awareness; Design and evaluation; digital safety; Intervention design; Pre-service teachers

1. Introduction

Digital technologies have become integral to teaching, learning, administration and assessment in Nigerian educational institutions. However, the increasing reliance on digital platforms has heightened exposure to cybersecurity threats, including phishing, identity theft and ransomware. Although technical safeguards are essential, effective cybersecurity also depends on users' awareness, knowledge and behaviour (Furnell & Clarke, 2012; Parsons *et al*., 2014).

Colleges of Education are strategically positioned to enhance cybersecurity awareness, as their graduates become future educators and advocates of responsible digital practices. Consequently, integrating cybersecurity education into teacher preparation programmes can promote safer digital behaviour and strengthen

cybersecurity awareness across the education system (Quayyum *et al*., 2021). However, building on a previously proposed six-layer framework comprising education, training, communication, governance, partnership and evaluation.

This study focuses on the education and evaluation dimensions. It develops an eight-week cybersecurity awareness module and proposes an evaluation protocol for assessing its effectiveness in a Nigerian College of Education. Moreover, recent evidence further demonstrated the structured, interactive and continuous cybersecurity training that can improve users' security behaviour (Prümmer *et al*., 2024). Accordingly, the study examines the module's effectiveness through a practical, resource-conscious evaluation design, with testable hypotheses to support empirical validation and future application in Nigerian teacher education institutions.

2. Background

2.1 Bridging the Gap Between Cybersecurity Awareness and Responsible Digital Behaviour

Awareness is commonly understood as knowledge, attitudes and behaviour (Kruger & Kearney, 2006), but knowing about threats does not reliably produce safe practice. Campaigns often fail because they inform without motivating and ignore the context in which people work (Bada et al., 2019; Cain et al., 2018). Four theoretical mechanisms inform the module. Protection Motivation Theory attributes protective behaviour to threat appraisal and coping appraisal (Rogers, 1975). Self-efficacy determines whether people act on what they know (Bandura, 1977). The Theory of Planned Behaviour adds the influence of subjective norms and perceived control (Ajzen, 1991; Ifinedo, 2012). The Technology Acceptance Model implies that cumbersome controls are bypassed, so secure options must be easy to use (Davis, 1989).

2.2 The Nigerian College of Education context

Nigeria has a substantial legal and policy base, including the Cybercrimes (Prohibition, Prevention, etc.) Act (Federal Republic of Nigeria, 2015), the Nigeria Data Protection Act (Federal Republic of Nigeria, 2023) and the National Cybersecurity Policy and Strategy (Federal Ministry of Communications and Digital Economy, 2021). Evidence on how these instruments translate into school-level practice is thin, and published, context-specific intervention designs for teacher trainees are scarce. Everyday risks likely to be salient for trainees include mobile-money fraud, scam links on messaging platforms, shared devices and accounts, and fraudulent result-checking or scholarship offers.

2.3 Cybersecurity threats and vulnerabilities in Nigerian Colleges of Education.

Educational institutions worldwide are increasingly exposed to cybersecurity threats due to open and decentralized networks, diverse user populations, bring-your-own-device (BYOD) practices, limited financial resources and the need for information sharing (Cisco & Talos, 2025). Common threats affecting the education sector include phishing attacks targeting staff and students, ransomware disrupting administrative and learning systems, identity theft, unauthorized access to examination records and the compromise of online learning platforms (Sophos, 2025). However, these threats can result in compromised accounts, loss of access to institutional systems, unauthorized disclosure of personal information, disruption of teaching and assessment, and financial and reputational damage. Such vulnerabilities highlight the need for proactive cybersecurity education and institutional preparedness in Nigerian Colleges of Education. These risks are discussed as potential threats requiring investigation and prevention, rather than as documented incidents in Nigerian Colleges of Education.

Emerging digital technologies are creating new cybersecurity challenges for pre-service teachers. Generative artificial intelligence (AI) has made it easier for cybercriminals to develop convincing and personalised phishing messages, reducing the reliability of traditional warning signs such as spelling and grammatical errors. Consequently, cybersecurity training should emphasise sender authentication, verification of suspicious

requests and the use of trusted communication channels. Similarly, mobile banking and financial fraud, including SIM-swap attacks, fake transaction alerts and identity impersonation, pose potential risks to students and staff who depend on digital financial services. Informal use of messaging platforms, particularly WhatsApp and Telegram, also increases exposure to fraudulent links, social engineering and account compromise. Furthermore, sharing personal or institutional information through unsecured online platforms, including AI-powered applications, may result in data leakage, while shared devices and accounts increase the risk of credential exposure and unauthorised access. Individual online habits and impulsive digital behaviour may further influence cybersecurity practices (Hadlington, 2017). These challenges highlight the importance of integrating practical digital safety skills, responsible technology use and behavioural awareness into teacher preparation programmes.

Young people are particularly vulnerable to online threats. According to Quayyum *et al.* (2021), in a systematic review of cybersecurity awareness among children, identified concerns relating to harmful online content, cyberbullying, privacy violations and internet fraud, while highlighting inconsistencies in the design and evaluation of awareness interventions. Since teachers play a significant role in shaping pupils' digital knowledge and behaviour, strengthening cybersecurity awareness among pre-service teachers is essential. Inadequate preparation at this level may consequently limit the effective transfer of safe digital practices to future generations of learners.

2.4 Barriers to effective awareness building

The companion review identified seven interrelated barriers that commonly limit awareness programmes in resource-constrained educational settings: limited resources, a shortage of dedicated staff, policy gaps, complacency, a weak reporting culture, the gap between knowledge and behaviour, and fragmented coordination. These are analytical categories derived from the literature and not measured findings about Nigerian institutions. They reinforce one another: limited resources reduce the capacity to hire and train staff, the absence of staff and policy leaves awareness without an owner, and complacency weakens demand for improvement. Three of them bear directly on module design. Complacency calls for local, realistic scenarios that build perceived vulnerability. A weak reporting culture calls for practising blame-free reporting. The knowledge–behaviour gap calls for hands-on practice paired with usable tools. It would also be unhelpful to treat trainees as the weakest link; security that ignores how people actually work is likely to fail, and the more productive approach is to treat users as partners (Sasse et al., 2001).

2.5 Rationale and gap

Although general awareness models and instruments exist, they were mostly developed in settings with different infrastructure, funding and institutional culture. For Nigerian colleges of education there is little published guidance that links theory, national law and classroom activity in a form that a lecturer can teach and a researcher can test. This paper addresses that gap by specifying a module and an evaluation that are explicit about their assumptions, so that others can examine, criticise and improve them.

3. Module Design

3.1 Design principles

The module follows five principles drawn from the framework: role relevance, motivation rather than information alone, leadership and norms, usability, and continuity. In practice this means short lectures followed by hands-on activities, local and realistic scenarios, tools that trainees can use on their own phones, a blame-free approach to mistakes (Sasse *et al.*, 2001), and a final week in which trainees learn to teach the topic to pupils.

3.2 Structure

The module runs for eight weeks, with one session of about two hours per week inside an existing computer literacy or ICT course. Table 1 maps each week to a behavioural domain adapted from the HAIS-Q (Parsons et al., 2014) and to the main mechanism it targets.

Table 1. Module structure, behavioural domains and target mechanisms

Week	Topic	HAIS-Q domain	Core activity and target mechanism
1	Why cybersecurity matters in education	Cross-cutting	Local case discussion; builds perceived vulnerability and severity (PMT)
2	Phishing, malware and scams	Email use; internet use	Sorting genuine and fraudulent messages; builds threat recognition and self-efficacy
3	Passwords and account protection	Password management	Create passphrases; set up multi-factor authentication; builds self-efficacy and ease of use (TAM)
4	Devices, networks and public Wi-Fi	Mobile device use	Checklist audit of a personal device; builds perceived control (TPB)
5	Protecting student and staff data	Information handling	Classify sample records; practise safe sharing; links to the Data Protection Act
6	Online conduct, privacy and cyberbullying	Social media use	Role play on responding to harassment; builds norms and coping skills
7	Law, policy and reporting incidents	Incident reporting	Mock incident report through a blame-free channel; builds reporting norms
8	Teaching cybersecurity to pupils	Cross-cutting	Design and deliver a short age-appropriate lesson; consolidates self-efficacy

3.3 Delivery in low-resource settings

The module is designed to run without specialized infrastructure. Activities use printed or projected examples and trainees' own phones, and no software purchase is required. Sessions can be repeated offline during power or bandwidth interruptions. A short facilitator guide, slide set and set of scenario cards would be prepared by the institution's ICT staff or an ICT champion, which also builds internal capacity.

3.4 Week-by-week session plans

Each session follows a common pattern: a ten-minute recap and warm-up, a short input of about twenty minutes, a practical activity of about fifty minutes, and a closing reflection with a take-home action. The plans below give the learning objectives, content and activity for each week.

Week 1: Why cybersecurity matters in education. By the end of the session, trainees should be able to explain why schools and colleges are targeted, name the kinds of data an institution holds, and describe how one incident could affect teaching, assessment and pupils. The input covers the threat landscape and the value of student data. In the activity, small groups read a short, realistic scenario about a compromised staff mailbox and trace its consequences on a simple impact map. The aim is to build perceived vulnerability and severity, countering the belief that educational institutions are unlikely targets.

Week 2: Phishing, malware and scams. Trainees should be able to recognise common signs of fraudulent messages, verify a sender and a request through a second channel, and describe what to do after clicking a suspicious link. The input introduces phishing, malware and social engineering, emphasising trust, urgency and authority as the levers attackers use (Hadnagy, 2018). In the activity, trainees sort a set of printed or projected messages into genuine and fraudulent, including fake scholarship offers, result-checking links, mobile-money

alerts and messages that mimic an official. Discussion focuses on the cues used and on cases where the cues were misleading.

Week 3: Passwords and account protection. Trainees should be able to create a strong passphrase, explain why passwords should not be reused or shared, and enable multi-factor authentication on an account of their choice. The input is short, because most of the session is hands-on. Trainees set up multi-factor authentication on their own email or messaging account with facilitator support. The activity is designed to build self-efficacy and to show that secure options can be easy to use.

Week 4: Devices, networks and public Wi-Fi. Trainees should be able to audit their own device against a checklist covering screen lock, updates, security software, app permissions and backups, and to explain the risks of public Wi-Fi and shared computers. Trainees complete the checklist individually, then agree on three improvements they will make during the week. Pirated software and unpatched devices are discussed as practical risks rather than moral failings.

Week 5: Protecting student and staff data. Trainees should be able to classify examples of data as public, internal or confidential, identify obligations under the Nigeria Data Protection Act (Federal Republic of Nigeria, 2023), and describe safe ways of sharing results and records. In the activity, trainees classify a set of sample records and decide what may be shared over messaging platforms and what may not. Particular attention is paid to the data of children and to the risks of uploading personal data to online tools.

Week 6: Online conduct, privacy and cyberbullying. Trainees should be able to describe the risks of oversharing on social media, recognise cyberbullying and harassment, and respond appropriately as a teacher. The activity is a role play in which trainees practise responding to a pupil who reports harassment. Ground rules for confidentiality and respect are agreed at the start, and the facilitator should be prepared to refer participants to institutional support services.

Week 7: Law, policy and reporting incidents. Trainees should be able to outline the purpose of the Cybercrimes Act (Federal Republic of Nigeria, 2015) and the Data Protection Act, describe a basic institutional policy, and complete an incident report. The input presents a simple policy outline, and the activity is a mock incident exercise in which trainees report a suspicious message through a blame-free channel. The aim is to normalise early reporting and to reduce the fear of blame that discourages disclosure (Reason, 1990; Sasse et al., 2001).

Week 8: Teaching cybersecurity to pupils. Trainees should be able to design and deliver a short, age-appropriate lesson on one topic from the module. Working in pairs, they select a topic, an age group and a learning objective, prepare a ten-minute lesson, and deliver it to peers, who give structured feedback. The session consolidates learning by teaching and links directly to the multiplier role of colleges of education.

3.5 Facilitator preparation and materials

The module is most likely to succeed when the facilitator is confident and the materials are simple. A facilitator should complete the activities personally before teaching them, prepare a printed pack of scenario cards and message examples drawn from local experience, and agree with the institution on a reporting channel that trainees can use in week 7. A half-day preparation workshop is suggested. Materials should be reviewed each cycle so that examples remain current, because the threat landscape changes quickly.

3.6 Adaptation to other settings

The module is written for NCE trainees but can be adapted. For secondary schools the weeks can be shortened and the vocabulary simplified, with greater emphasis on safe social media use and cyberbullying. For in-service teachers the content can be compressed into workshops with refresher sessions at least annually. Where only a few sessions are available, weeks 2, 3, 5 and 7 are suggested as the core, because they address phishing, account protection, data handling and reporting.

4. Evaluation Protocol

4.1 Research questions and hypotheses

The pilot study addresses three questions. **RQ1:** Does the module improve cybersecurity knowledge, attitudes and self-reported behaviour among teacher trainees compared with trainees who receive no module? **RQ2:** Does the module improve the ability to recognise phishing messages and self-efficacy? **RQ3:** Are any gains retained after a delay? The hypotheses are:

- **H1:** Trainees who complete the module will show greater gains in HAIS-Q knowledge, attitude and behaviour scores than the comparison group.
- **H2:** Trainees who complete the module will show greater gains in phishing-recognition accuracy than the comparison group.
- **H3:** Gains in self-efficacy will be larger in the module group, and will be positively associated with gains in self-reported behaviour (consistent with Proposition P6 of the companion review).
- **H4:** At a delayed follow-up, the module group will retain a significant part of its gains relative to baseline.

4.2 Design

A quasi-experimental pretest–posttest design with a non-equivalent comparison group is proposed, because random assignment of individuals is usually impractical inside intact classes. Whole classes or course sections in the same college are assigned to the module group or to a comparison group that follows the normal syllabus. The comparison group is offered the module after the delayed follow-up, so that no trainee is denied the benefit. Measurements are taken at baseline (week 0), immediately after the module (week 9) and at follow-up about eight weeks later.

4.3 Participants and sample size

Participants are NCE trainees enrolled in a computer literacy or ICT course. For a two-group comparison of change scores, detecting a medium effect ($d = 0.5$) at a significance level of 0.05 with 80% power requires about 64 participants per group. Allowing for roughly 20% attrition, the target is about 80 per group. Where fewer trainees are available, the study should be reported as exploratory and the effect sizes interpreted with caution.

4.4 Measures

Table 2 lists the measures. The HAIS-Q items should be adapted to local devices, platforms and language and checked for clarity with a small group of trainees before use. Self-reported behaviour is subject to social desirability bias, which is why behavioural tasks are included.

Table 2. Outcome measures

Construct	Instrument	Timing
Knowledge, attitudes and self-reported behaviour	Adapted HAIS-Q (Parsons et al., 2014), seven domains	Baseline, post, follow-up
Phishing recognition	Set of 12 realistic messages (half genuine, half fraudulent) classified by trainees; accuracy and confidence recorded	Baseline, post, follow-up
Self-efficacy	Short scale on confidence in tasks such as spotting a fake login page and setting up multi-factor authentication (Bandura, 1977)	Baseline, post, follow-up
Threat appraisal	Items on perceived severity and vulnerability (Rogers, 1975)	Baseline, post

Construct	Instrument	Timing
Module reaction	Brief satisfaction and relevance questionnaire (first Kirkpatrick level; Kirkpatrick & Kirkpatrick, 2006)	Week 8

4.5 Procedure

The procedure has five steps: (1) obtain institutional permission and prepare materials; (2) pilot and refine the instruments; (3) administer the baseline measures to both groups; (4) deliver the module to the module group over eight weeks; and (5) administer the post-test and the delayed follow-up. The same facilitator should teach all module sessions, and attendance should be recorded so that dose of exposure can be examined.

4.6 Analysis plan

Internal consistency of each scale will be reported with Cronbach's alpha. Group equivalence at baseline will be checked, and differences in change scores will be tested using analysis of covariance with the baseline score as covariate (or a mixed-design analysis of variance across the three time points), reporting effect sizes and confidence intervals. The association between self-efficacy gains and behaviour gains (H3) will be examined through correlation or regression. Missing data and attrition will be reported, and the analysis will state whether it is by intention to treat or by completion.

4.7 Threats to validity

The main threats are non-equivalence of groups, contamination between groups who share a campus, testing effects from repeated measures, reliance on self-report, and a facilitator effect. The design mitigates these through baseline adjustment, behavioural tasks, a delayed follow-up and a request that trainees do not share module materials until the study ends. Results from a single college cannot be generalised to all Nigerian institutions.

4.8 Ethical considerations

Because the study involves human participants, it requires institutional ethical approval before data collection, voluntary informed consent, and the right to withdraw at any time without penalty. Responses should be anonymised using codes, stored securely and reported only in aggregate. The phishing-recognition task must use fictitious messages and must not collect real credentials. Participation and results must not affect course grades.

4.9 Implementation timeline

Table 3 gives an indicative timeline of about seven months for one institution. It can be shortened if the instruments are already available, or extended to span an academic semester.

Table 3. Indicative timeline for the pilot study

Phase	Activities	Approximate duration
Preparation	Ethical approval; institutional permission; preparation of materials and facilitator workshop	4 weeks
Instrument pilot	Adapt HAIS-Q items; test clarity with a small group; refine the phishing task	2 weeks
Baseline	Administer baseline measures to both groups	1 week
Delivery	Eight-week module for the module group; normal teaching for the comparison group	8 weeks
Post-test	Administer post-test measures and the reaction questionnaire	1 week

Phase	Activities	Approximate duration
Follow-up	Delayed follow-up measures about eight weeks after the post-test	1 week (after 8-week gap)
Analysis and reporting	Data cleaning, analysis, reporting; offer module to the comparison group	6 weeks

4.10 Data management

Questionnaires should be completed on paper or on a secure institutional platform, using participant codes instead of names. A single master list linking codes to names should be stored separately from the data, accessible only to the lead researcher, and destroyed when the study ends. Data files should be kept in a password-protected, encrypted location with a backup following the 3-2-1 principle, consistent with the practices the module itself teaches. Data should be reported in aggregate, and small cells that could identify individuals should be suppressed.

4.11 Dissemination and use of results

Results should be shared first with the participating institution and with trainees, in plain language. They should then be reported to academic audiences, whether positive, negative or inconclusive, so that the evidence base is not biased towards successes. The module materials, instruments and a data-free analysis script could be released with the report to support replication in other colleges.

5. Discussion

If the hypotheses are supported, the module offers a low-cost route for embedding cybersecurity awareness in teacher preparation, and the evaluation would provide local evidence on which components matter most. If they are not supported, the pattern of results would still be informative. For example, gains in knowledge without gains in behaviour would support the argument that awareness must be paired with usable tools and supportive norms (Bada et al., 2019), pointing to the governance and technical layers of the framework. Results would also help refine the six propositions in the companion review and guide adaptation to other settings, such as secondary schools or in-service training.

5.1 Limitations

This is a design paper. It reports no empirical results, and the module has not yet been tested. The sample size calculation assumes a medium effect that may not be realistic, the instruments need local validation, and the proposed design cannot establish causality as firmly as a randomised trial. Much of the supporting evidence comes from settings that differ from Nigerian colleges, so transferability must be tested.

6. Conclusion

Teacher trainees are a high-leverage group for cybersecurity awareness in Nigeria. This paper has set out an eight-week module that links activities to behavioural domains and theoretical mechanisms, and a feasible protocol for evaluating it. Implementation of the pilot, and publication of its results whether positive or negative, are the next steps. Colleges of education, teacher educators and policymakers are invited to adapt the module and share findings so that the evidence base for Nigerian education can grow.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36–45.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Federal Ministry of Communications and Digital Economy. (2021). *National cybersecurity policy and strategy 2021*. Federal Republic of Nigeria.

Federal Republic of Nigeria. (2015). *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015*. Official Gazette.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. Official Gazette.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95.

Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating training programs: The four levels* (3rd ed.). Berrett-Koehler.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585.https://doi.org/10.1016/j.cose.2023.103585

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 100343.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122–131.

Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2024). A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness. Journal of Systems and Software, 208, 111899. https://doi.org/10.1016/j.jss.2023.111899