

Cybersecurity Awareness, Everyday Practices and Privacy Behaviour among Students of the University of Lagos: A Survey-Based Case Study

OKOLO, Chuks Emmanuel

chuksokoloe@gmail.com

<https://chuks.is-a.dev>

<https://orcid.org/0009-0007-2514-3744>

Published: 24 October 2026

Abstract

Nigerian students do their banking, learning, borrowing and socialising on the same phone, which makes them easy and frequent targets for online fraud. This article reports an anonymous online survey of 384 students of the University of Lagos, drawn from undergraduate and postgraduate levels, on what they know about cybersecurity, what they actually do, what has happened to them, and what they expect from the university. Knowledge was uneven. Nearly everyone (99.2%) knew that a bank never asks for an OTP, yet fewer than half answered correctly on password reuse (26.3%), the padlock icon (23.7%), public Wi-Fi (29.2%) and antivirus software (45.8%). The same pattern showed in behaviour: 99.2% lock their devices and 95.1% never share OTPs, but 78.6% often use their school password on other sites and 92.2% sometimes use public Wi-Fi for banking. Incident exposure was high, with 62.2% reporting loan-app harassment, 54.9% a phishing or scam message and 26.6% money lost to online fraud. Almost all respondents (99.5%) had seen a deepfake, while 2.9% felt able to tell AI-written scam messages from genuine ones. Some 99.2% asked for more training. Six structured problems and matching recommendations are set out. The data are self-reported, cross-sectional and drawn from a convenience sample, so the results describe stated knowledge and habits, not measured security outcomes.

Keywords: cybersecurity awareness; phishing; password reuse; privacy; higher education; Nigeria; loan apps; deepfakes

1. Introduction

A student in Lagos can pay school fees, receive a scholarship alert, apply for a loan and be scammed on the same phone within the same hour. That ordinary scene is the setting for this article.

Security researchers have said for years that the weakest link in most breaches is a person and not a machine. Verizon's annual breach investigations keep finding that a human element, such as a click, a reused password or a misdirected message, features in a large share of incidents (Verizon, 2024). University students sit in a particularly exposed position. They are young, heavy users of mobile services, often handling money for the first time, and they carry identity documents, bank apps and school credentials on a single device.

Most of the research on how people behave online comes from North America and Europe (Ion et al., 2015; Egelman & Peer, 2015). Evidence from Nigerian public universities is thin, even though the country has passed a data protection law (Federal Republic of Nigeria, 2023) and regulators have moved against abusive digital lenders (Channels TV, 2025). This study adds a data point from one large public university in Lagos.

The article asks four questions. RQ1: how much do students know about core cybersecurity ideas? RQ2: how consistently do they apply safe practices and protect their privacy? RQ3: what incidents have they met, and what did those cost? RQ4: how do they see the university's role, and how ready are they for newer, AI-related threats? A word on scope. The analysis is descriptive. I worked from item-level tallies and not individual records, so I cannot test relationships between answers, and the findings should be read with that in mind.

2. Context

The University of Lagos is a large public university in Lagos, Nigeria's biggest city and its commercial centre. For students in that environment, the phone is the main computer. In this survey 98.2% named a smartphone as their main device for study and banking, and 55.7% said their main route to the internet is mobile data (Table 1).

Two features of the Nigerian setting matter for the questions asked here. The first is law. The Nigeria Data Protection Act 2023 created the Nigeria Data Protection Commission and gave individuals rights over their personal data, among them access, correction and erasure, while placing duties on organisations that handle it (Federal Republic of Nigeria, 2023; KPMG Nigeria, 2023). The second is digital lending. Loan apps have been accused for several years of harassing borrowers and contacting their friends and family. The Federal Competition and Consumer Protection Commission (FCCPC) responded with a registration framework and later with the Digital, Electronic, Online or Non-Traditional Consumer Lending Regulations, which took effect in July 2025 and prohibit harassment and unethical debt recovery (Channels TV, 2025). Reporting from earlier in the process suggests that some lenders carried on contacting borrowers' contacts despite the rules (Nairametrics, 2023). That history is why the questionnaire asked about loan-app harassment as a distinct experience.

3. Review of the Literature

3.1 *People, not only machines*

Wash (2010) showed that ordinary users reason about security through informal "folk models" of hackers and viruses. These models can be reasonable and still lead people to rely on one protection while neglecting another. Ion et al. (2015) compared experts with non-experts and found a telling difference: non-experts leaned heavily on antivirus software, while experts emphasised software updates, password managers and two-factor authentication. Egelman and Peer (2015) built a scale for self-reported security behaviour that covers securing devices, choosing passwords, staying alert and updating software, which is the same ground covered by the practice items in this study's questionnaire.

3.2 *Passwords and reuse*

Das et al. (2014) found that people reuse passwords, or tweak them only slightly, across sites, and that this makes cross-site guessing practical for an attacker who has obtained one password. Current guidance from

the US National Institute of Standards and Technology favours long passwords or passphrases over complicated short ones, and recommends screening new passwords against lists of known breached ones (Grassi et al., 2017). Reuse matters most for credentials that unlock something valuable, which includes an email account, a bank profile or a student portal.

3.3 Phishing and what works against it

Dhamija et al. (2006) tested how people judge websites and found that well-made fake sites fooled a large majority of participants, partly because people ignored or misread browser security cues. That finding bears on the belief that a padlock icon proves a site is safe. Sheng et al. (2010) reported that younger adults were more susceptible to phishing than older ones and that educational material reduced the risk. Kumaraguru et al. (2010) found that embedded, learn-by-doing training, delivered when a person falls for a simulated phish, helped people resist later attempts. Scammers also lean on well-known persuasion levers such as authority and urgency (Cialdini, 2009), which is the logic of the fake bank call and the "your account closes in 24 hours" message.

3.4 Privacy concern versus privacy behaviour

Studies of the so-called privacy paradox find that people often state concern about their personal data and still disclose it freely (Norberg et al., 2007). Acquisti et al. (2015) argue that privacy choices are shaped by context, uncertainty and convenience, so stated concern is a poor guide to what people actually do. This is relevant to items on location sharing and on sending ID documents through chat apps.

3.5 Motivation to protect oneself

Protection motivation theory holds that people protect themselves when they judge a threat to be serious and likely, and when they believe they have an effective response they can carry out (Rogers, 1975). A population that feels threatened but lacks confidence in its responses will not necessarily act, which is a useful lens for the training demand reported later.

3.6 AI-enabled deception

Chesney and Citron (2019) describe deepfakes, which are synthetic audio, images and video of real people, as a growing risk to privacy, trust and security, because they make impersonation cheaper and more convincing. For students, the practical risks include cloned voices, fake video calls and scam messages written fluently by language models.

3.7 Self-report has limits

Self-reported behaviour tends to be flattering, especially on socially approved actions (Nederhof, 1985), and answers gathered with one method from one source can be biased in shared ways (Podsakoff et al., 2003). People also tend to overrate their own competence in areas where they know little (Dunning & Kruger, 1999). I return to these cautions when interpreting the results.

4. Research Design and Method

Design and case. The study is a cross-sectional descriptive survey of one institution, the University of Lagos. A single case cannot support statistical generalisation, but it can yield grounded findings that other institutions can compare with their own (Yin, 2018). A survey suits the aim of describing attitudes and stated behaviour at one point in time (Creswell & Creswell, 2018).

Instrument. The questionnaire had 62 items in ten sections: consent and eligibility; background; a ten-item knowledge quiz (true, false or not sure); eleven practice items on a frequency scale; privacy attitudes; incidents and reporting (optional); awareness and the institution's role; AI-related threats; confidence and attitudes; and two open questions. Attitude items used a five-point agreement scale in the manner of Likert (1932). The full item list is in Appendix A.

Sampling and administration. The questionnaire was published as a Google Form and remained open for 7 days. The link was shared through official student channels. Participation was by convenience, which is practical but means respondents are those who were reachable and willing (Etikan et al., 2016). The target was 384 completed responses, the figure that gives a 5% margin of error at 95% confidence for a large population under Cochran's (1977) formula, and 384 students consented and completed the form.

Ethics and consent. The study received an ethics exemption from the University of Lagos Research Ethics Committee (UNILAGREC), reference UNILAGREC/2026/136547. The first page of the form explained the purpose, the voluntary nature of participation, the right to stop at any time, and the anonymity of answers. Respondents had to agree to take part (item A1) and confirm they were 18 or older and enrolled at the university (item A2); all 384 did so. The survey did not ask for names, matriculation numbers, contact details, passwords or account numbers, and the incident section was optional. Raw responses were to be held only for the analysis period of about three weeks and then deleted, in line with the protocol.

Analysis. Responses were tallied item by item. All percentages in this article are shares of the 384 respondents. Where the recorded counts for an item add up to fewer than 384, the remainder is shown as "not recorded", so percentages are conservative lower bounds. Multi-select items (B8, F1, F3, F4, F5, G1, G6) can add up to more than 100%.

Data notes. I want to be open about several quirks in the tallies, because they affect how far the results can be pushed.

- Counts for many items add up to fewer than 384, and for several items only some answer categories were tallied. No counts were available for items E1, E2, E3, G4, H4 and J2, for most categories of F3 and F4, or for several options in F1 and G1, so those results are not reported.
- Item B3 records no respondents aged 21 to 24, and two answers are missing, which is unusual in a sample of whom 68.2% were in the first two years of an undergraduate programme. Item B2 records only four fields of study, with none in science and technology, the arts or law. Both may be tallying issues or true features of who responded.
- In item F2, 112 respondents are recorded as having lost money (in three loss bands), while only 102 selected "money lost to online fraud" in item F1. I report both as recorded.
- Item B8 records no counts for loan apps, although 239 respondents reported loan-app harassment in item F1.
- Because I worked from tallies and not from individual records, I could not cross-tabulate answers, compute scores for each respondent, test differences between groups, or check the reliability of scales.

5. Findings

5.1 Who answered

Table 1 shows the profile. Most respondents (68.2%) were undergraduates in the first two years, 21.6% were in Year 3 or above, and 10.2% were postgraduates. Women made up 59.1%. Half the sample (49.2%) were in health sciences and about a third (32.3%) in education, so the findings lean towards those fields. Almost all (98.2%) used a smartphone as their main device, mobile data was the main route to the internet for 55.7%, and two thirds (66.4%) spent two to four hours online a day.

Item	Recorded answers: count (% of 384)
Level of study (B1)	Undergraduate, Year 1-2 262 (68.2%); Undergraduate, Year 3 and above 83 (21.6%); Postgraduate (diploma, master's, PhD) 39 (10.2%)
Field of study (B2)	Health sciences 189 (49.2%); Education 124 (32.3%); Social and management sciences 48 (12.5%); Engineering 23 (6.0%)
Age group (B3)	18-20 183 (47.7%); 25-30 152 (39.6%); 31-40 47 (12.2%); not recorded 2 (0.5%)
Gender (B4)	Female 227 (59.1%); Male 157 (40.9%)
Main device (B5)	Smartphone 377 (98.2%); not recorded 7 (1.8%)
Main internet source (B6)	Mobile data 214 (55.7%); Campus Wi-Fi 89 (23.2%); Home broadband 81 (21.1%)
Hours online per day (B7)	2-4 hours 255 (66.4%); 5-8 hours 101 (26.3%); Under 2 hours 28 (7.3%)
Services used regularly (B8, multi-select)	Mobile banking or fintech 202 (52.6%); Social media 189 (49.2%); School portal or e-learning 110 (28.6%); Online shopping 87 (22.7%)

Table 1. Respondent profile ($N = 384$). See Section 4 for notes on B3, B2 and B8.

5.2 What students know

Table 2 gives the ten knowledge items. The average share of correct answers across items was 57.3% (2,199 correct answers out of a possible 3,840), equal to a mean of about 5.7 out of 10 if every respondent had been scored. That figure is a lower bound, because unrecorded answers count as not correct. The spread across items matters more than the average. Students were strong on the points that are drilled into Nigerians by banks and in public campaigns: 99.2% knew that a bank will never ask for an OTP or PIN (C5), 83.6% knew that two-factor authentication still protects an account when a password is stolen (C4), and 74.7% knew that phishing is not limited to email (C6). Two thirds (66.4%) were suspicious of an urgent "your account will close" message (C9).

Four items fell below half. Only 26.3% knew that a long password does not make reuse safe (C1), 23.7% knew that a padlock icon does not guarantee a genuine site (C2), 29.2% knew that public Wi-Fi can expose activity to others (C3), and 45.8% knew that antivirus alone does not protect against every threat (C8). On C1, C2 and C3 together, 236 answers were "not sure", which suggests honest uncertainty and not only error. A majority actually chose the wrong answer on C1 (55.7% said reuse is safe if the password is long), C2 (51.0% trusted the padlock), C3 (52.1% said public Wi-Fi does not expose activity) and C8 (51.8% said antivirus protects against everything). These match the kind of misplaced trust in a single protection described by Wash (2010) and Ion et al. (2015).

Item	Correct answer	Correct: n (%)	Other answers: n (%)	Not recorded
C1 Long password makes reuse safe	False	101 (26.3%)	True 214 (55.7%); Not sure 69 (18.0%)	0
C2 Padlock guarantees a genuine site	False	91 (23.7%)	True 196 (51.0%); Not sure 97 (25.3%)	0

Item	Correct answer	Correct: n (%)	Other answers: n (%)	Not recorded
C3 Public Wi-Fi can expose activity	True	112 (29.2%)	False 200 (52.1%); Not sure 70 (18.2%)	2
C4 Two-factor still protects a stolen password	True	321 (83.6%)	False 61 (15.9%)	2
C5 Bank never asks for OTP or PIN	True	381 (99.2%)	None recorded	3
C6 Phishing happens only by email	False	287 (74.7%)	True 95 (24.7%)	2
C7 Updates fix known weaknesses	True	212 (55.2%)	False 168 (43.8%)	4
C8 Antivirus alone protects against all threats	False	176 (45.8%)	True 199 (51.8%)	9
C9 Urgent account-closure message is suspicious	True	255 (66.4%)	False 127 (33.1%)	2
C10 Apps from outside the store are riskier	True	263 (68.5%)	False 121 (31.5%)	0

Table 2. Cybersecurity knowledge ($N = 384$). Percentages are of all 384 respondents.

5.3 What students do

Table 3 shows the practice items. Some good habits are close to universal: 99.2% always lock their phone or laptop (D10), 95.1% say they never share an OTP, PIN or password (D7), and 76.8% often use two-factor authentication on email and banking (D3). A majority (75.0%) always back up important files (D9).

The weaker habits are those where knowledge was also weak. No respondent said they often or always use a different password for each important account (D1): 51.8% said rarely and 48.2% sometimes. Among the 296 who answered the password-length item, 211 (54.9% of the sample) said they never use long passwords or passphrases (D2). A striking 78.6% often use their school email or portal password on other websites (D11). Public Wi-Fi is used sometimes for banking or other important logins by 92.2% (D6), and 75.3% sometimes install apps from outside the official store (D8). Updates are installed promptly only sometimes by those who answered (D4, 77.3%). Only 15.4% always check the sender and the link before acting on an urgent message (D5), while 75.0% do so sometimes.

Item	Safe direction	Recorded answers: n (% of 384)	Not recorded
D1 Different password for each key account	Higher is safer	Rarely 199 (51.8%); Sometimes 185 (48.2%)	0 (0.0%)
D2 Long passwords or passphrases	Higher is safer	Never 211 (54.9%); Sometimes 85 (22.1%)	88 (22.9%)
D3 Two-factor authentication on email and banking	Higher is safer	Often 295 (76.8%); Sometimes 80 (20.8%)	9 (2.3%)
D4 Install updates promptly	Higher is safer	Sometimes 297 (77.3%)	87 (22.7%)
D5 Check sender and link before acting	Higher is safer	Always 59 (15.4%); Sometimes 288 (75.0%)	37 (9.6%)
D6 Use public Wi-Fi for banking or key logins	Lower is safer	Rarely 12 (3.1%); Sometimes 354 (92.2%)	18 (4.7%)
D7 Share an OTP, PIN or password	Lower is safer	Never 365 (95.1%)	19 (4.9%)
D8 Install apps from outside the official store	Lower is safer	Never 21 (5.5%); Sometimes 289 (75.3%)	74 (19.3%)
D9 Back up important files	Higher is safer	Always 288 (75.0%); Sometimes 68 (17.7%)	28 (7.3%)
D10 Lock phone or laptop	Higher is safer	Always 381 (99.2%)	3 (0.8%)

Item	Safe direction	Recorded answers: n (% of 384)	Not recorded
D11 Reuse school password on other sites	Lower is safer	Never 23 (6.0%); Often 302 (78.6%)	59 (15.4%)

Table 3. Security practices ($N = 384$). Scale: never, rarely, sometimes, often, always. Categories with no recorded count are omitted.

5.4 Privacy attitudes

Table 4 covers privacy. Over half (54.9%) agreed that they often share their location publicly on social media (E4), and 74.0% agreed they would send a photo of an ID card, BVN or NIN through a chat app if someone they trusted asked (E5). Those are the two items where agreement is the riskier answer. On the institution, 83.9% agreed that they trust it to protect their personal data (E6), yet only 57.6% agreed that they know what personal data it keeps about them (E7), and 26.8% disagreed. Awareness of the data protection law was shallow: 77.6% had heard of the Nigeria Data Protection Act 2023, and the counts for those who understand it well or have never heard of it were not recorded (E8).

Item	Recorded answers: n (% of 384)	Not recorded
E4 I often share my location publicly (agree is riskier)	Disagree 105 (27.3%); Agree 211 (54.9%)	68 (17.7%)
E5 I would send a photo of my ID, BVN or NIN through a chat app (agree is riskier)	Strongly disagree 91 (23.7%); Agree 284 (74.0%)	9 (2.3%)
E6 I trust my institution to protect my data	Agree 322 (83.9%)	62 (16.1%)
E7 I know what personal data my institution keeps	Disagree 103 (26.8%); Agree 221 (57.6%)	60 (15.6%)
E8 Understanding of the Nigeria Data Protection Act 2023	Have heard of it 298 (77.6%)	86 (22.4%)

Table 4. Privacy attitudes and behaviour ($N = 384$). No counts were available for E1, E2 and E3.

5.5 Incidents, losses and reporting

Table 5 shows that harmful experiences were common. In the previous 12 months, 62.2% had met harassment by a loan app or misuse of their contacts, 54.9% a phishing or scam message, 52.3% a fake call posing as a bank or school official, 48.7% malware or a virus, 31.5% a hacked social media or email account, and 26.6% had lost money to online fraud. Where loss bands were recorded, 55 respondents (14.3% of the sample) reported losing more than NGN 200,000, 32 (8.3%) between NGN 50,001 and 200,000, and 25 (6.5%) under NGN 5,000. As noted in Section 4, these loss counts total 112, slightly above the 102 who ticked money lost in F1, so they should be read as approximate.

Reporting looks thin, though the data are incomplete. Only the police category was tallied: 101 respondents (26.3%) said they reported an incident to the police. Counts for reporting to banks, to the university or to no one were not recorded, so I cannot say where most people turned or why many did not report. The threats students worry about most were account hacking (65.6%, F5) and loss of privacy on social media (54.7%), with online scams chosen by 22.7%. In the open question on the biggest problem, 52.3% named identity theft and 26.8% named impersonation (J1).

Experience in the last 12 months (F1, multi-select)	n	% of 384
Loan-app harassment or misuse of contacts	239	62.2%
Phishing or scam message	211	54.9%
Fake call posing as bank or school official	201	52.3%

Experience in the last 12 months (F1, multi-select)	n	% of 384
Malware or virus on my device	187	48.7%
Social media or email account hacked	121	31.5%
Money lost to online fraud	102	26.6%
Fake profile impersonating me	12	3.1%

Table 5. Incidents experienced ($N = 384$). No counts were available for school-portal misuse, online threats or blackmail, none, or prefer not to say.

Loss and reporting (F2, F3, F5)	n	% of 384
Lost under NGN 5,000	25	6.5%
Lost NGN 50,001 to 200,000	32	8.3%
Lost above NGN 200,000	55	14.3%
Reported to the police	101	26.3%
Top worry: account hacking	252	65.6%
Top worry: loss of privacy on social media	210	54.7%
Top worry: online scams	87	22.7%

Table 6. Losses, reporting and main worries ($N = 384$). The NGN 5,000 to 50,000 band had no recorded count. F5 allowed up to three choices.

5.6 The institution, AI threats and attitudes

Table 7 pulls together the remaining sections. Students mostly learn about online safety from social media (62.8%), with 13.3% saying their own reading. The university does not seem to feature: 71.4% were not sure whether it offers any cybersecurity training or orientation (G2). Even so, 84.6% agreed they know the institution has an IT or data-protection policy (G3), and two thirds (66.9%) found its systems secure, while 23.2% did not (G5). When asked what format would help most, 78.4% chose live workshops and 67.2% short videos, against 26.6% for an orientation module (G6).

AI-related threats are already part of student experience. Nearly all respondents (99.5%) had seen a deepfake or an AI-generated fake of a real person's face or voice (H1). Yet only 2.9% agreed they could tell an AI-written scam message from a genuine one, and 77.6% disagreed (H2). More than four in five (82.6%) said they at least rarely type sensitive information such as ID numbers, bank details or school records into AI chatbots (H3: rarely 78.6%, sometimes 3.9%).

Attitudes show motivation and some complacency side by side. Three quarters (75.0%) agreed they could become the target of a scam (I4), and 99.2% agreed they would like more training (I5, with 26.0% strongly agreeing). Some 83.6% said they would report a suspicious incident if they knew where to do so (I6). Against that, 67.2% agreed that online security is the IT department's job and not theirs (I2), and 53.4% agreed that measures such as strong passwords and two-factor authentication are too inconvenient (I3). A little over half (54.9%) said they feel confident they can recognise a phishing message, and 29.2% did not (I1).

Item	Recorded answers: n (% of 384)	Not recorded
G1 Main source of safety knowledge (up to 2)	Social media 241 (62.8%); My own reading 51 (13.3%)	92 (24.0%)
G2 Has institution offered training?	Not sure 274 (71.4%)	110 (28.6%)
G3 I know the institution has an IT or data policy	Agree 325 (84.6%)	59 (15.4%)

Item	Recorded answers: n (% of 384)	Not recorded
G5 Institution's systems feel secure	Disagree 89 (23.2%); Agree 257 (66.9%)	38 (9.9%)
G6 Preferred training format (up to 2)	Live workshops 301 (78.4%); Short videos 258 (67.2%); Orientation module 102 (26.6%)	-277 (-72.1%)
H1 I have seen a deepfake	Yes 382 (99.5%)	2 (0.5%)
H2 I can tell AI-written scams from genuine messages	Disagree 298 (77.6%); Agree 11 (2.9%)	75 (19.5%)
H3 I type sensitive data into AI chatbots	Rarely 302 (78.6%); Sometimes 15 (3.9%)	67 (17.4%)
I1 Confident I can recognise phishing	Disagree 112 (29.2%); Agree 211 (54.9%)	61 (15.9%)
I2 Security is IT's job, not mine (agree is riskier)	Strongly disagree 58 (15.1%); Agree 258 (67.2%)	68 (17.7%)
I3 Security measures are too inconvenient (agree is riskier)	Disagree 101 (26.3%); Agree 205 (53.4%)	78 (20.3%)
I4 I could become a scam target	Disagree 15 (3.9%); Agree 288 (75.0%)	81 (21.1%)
I5 I would like more training	Agree 281 (73.2%); Strongly agree 100 (26.0%)	3 (0.8%)
I6 I would report if I knew where	Agree 321 (83.6%)	63 (16.4%)

Table 7. Awareness, institution, AI threats and attitudes ($N = 384$). No counts were available for G4, H4 and the second open question (J2).

6. Structured Analysis of the Problems

The results point to six problems. For each, I set out the evidence, why it matters in light of the literature, and how firmly the data support it. Because I could not link answers to individual respondents, the connections I draw between items are patterns across the sample and not proof that the same students gave both answers.

Problem 1: Weak password hygiene, especially for school credentials

Evidence. Nobody reported often or always using a different password for each key account (D1). Among those who answered D2, most said they never use long passwords or passphrases. About four in five (78.6%) often reuse their school password elsewhere (D11), and only 26.3% knew that long passwords do not make reuse safe (C1). **Why it matters.** Reuse lets an attacker who obtains one password try it on other accounts (Das et al., 2014), and a student's school login can lead to a portal, an email inbox and personal records. Guidance now favours long passphrases and breach screening over complexity rules (Grassi et al., 2017). **Strength of support.** Strong. Several items point the same way.

Problem 2: Risky everyday habits around networks, apps and personal documents

Evidence. 92.2% sometimes use public Wi-Fi for banking or key logins (D6) while only 29.2% understood the exposure (C3). 75.3% sometimes install apps from outside the official store (D8). 54.9% share their location publicly (E4) and 74.0% would send an ID, BVN or NIN photo through a chat app (E5). Only 15.4% always check the sender and link of an urgent message (D5), and only 23.7% knew that a padlock icon proves nothing (C2). **Why it matters.** Each habit gives an attacker an opening, and the padlock belief is exactly the weak reliance on visual cues that Dhamija et al. (2006) documented. The ID-photo finding fits the privacy paradox, where people say they are worried yet act for convenience or trust (Norberg et al., 2007; Acquisti et al., 2015), although here E1 was not tallied so I cannot test stated concern directly. **Strength of support.** Strong for the habits, moderate for the explanation.

Problem 3: High exposure to fraud and harassment, large losses and thin reporting

Evidence. 62.2% met loan-app harassment, 54.9% a phishing or scam message, 52.3% a fake bank or school call, and 26.6% lost money, with 14.3% of the sample recording losses above NGN 200,000. Only 26.3% reported to the police; other channels were not tallied. **Why it matters.** Loan-app harassment persists despite regulation (Nairametrics, 2023; Channels TV, 2025), and fake-caller scams exploit authority and urgency (Cialdini, 2009). Heavy exposure and large losses suggest that awareness has not translated into protection. Low reporting hides the true scale from both the university and the authorities. **Strength of support.** Strong on exposure and loss, limited on reporting because most reporting categories were not tallied. The loss counts have the inconsistency noted in Section 4.

Problem 4: A gap between trust in the institution and what students know about it

Evidence. 83.9% trust the university to protect their data (E6), but only 57.6% know what data it holds (E7), 71.4% do not know whether it offers training (G2), and 67.2% think security is IT's job and not theirs (I2). Students mostly learn from social media (62.8%) and not from the institution. **Why it matters.** Trust without knowledge is fragile. Under the Nigeria Data Protection Act, individuals have rights over their data (Federal Republic of Nigeria, 2023; KPMG Nigeria, 2023), but only 77.6% had even heard of the Act, and the data do not show how many understand it. An institution that does not make its policy and its training visible cannot rely on students to follow it. The finding that 84.6% say they know a policy exists, while 71.4% are unsure about training, suggests awareness is shallow. **Strength of support.** Moderate. Several categories were not tallied, so the true spread is unclear.

Problem 5: AI-enabled deception is outpacing students' ability to spot it

Evidence. 99.5% have seen a deepfake, 2.9% feel able to tell AI-written scam messages from genuine ones (H2), and 82.6% at least rarely enter sensitive information into AI chatbots (H3). **Why it matters.** Deepfakes lower the cost of convincing impersonation (Chesney & Citron, 2019), which compounds problems 2 and 3. Students feel exposed and unable to detect, which in protection motivation terms means high threat perception with low confidence in their response (Rogers, 1975). Sharing sensitive data with chatbots adds a privacy risk of its own. **Strength of support.** Strong on perceived ability, moderate on behaviour, because H4 (using AI to check scams) had no counts.

Problem 6: Knowledge and practice rise and fall together, and training demand is untargeted

Evidence. Where knowledge is high, practice is strong: 99.2% knew that banks never ask for OTPs and 95.1% never share them; 83.6% knew two-factor authentication helps and 76.8% use it often. Where knowledge is low, practice is poor: password reuse (26.3% correct, D1 and D11 weak), public Wi-Fi (29.2% correct, 92.2% use it for banking), and antivirus (45.8% correct). Meanwhile 99.2% want more training, mostly in live workshops (78.4%) and short videos (67.2%). **Why it matters.** The pattern suggests that well-aimed teaching can change habits, as the training studies imply (Sheng et al., 2010; Kumaraguru et al., 2010), and that generic awareness talks would waste effort on topics students already know. It also hints at a mismatch between confidence and care: 54.9% feel confident of spotting phishing while only 15.4% always check sender and link, a gap of the kind Dunning and Kruger (1999) describe, though without respondent-level data I cannot show it holds for the same people. **Strength of support.** Moderate. This is a pattern across items and a plausible reading, not a tested relationship.

7. Recommendations

Each recommendation is tied to a problem above. They are suggestions for the university's consideration. The evidence for them is the survey combined with the cited literature, not a trial of the measures themselves.

Problem	Recommendation	Suggested owner	Timing
1 Passwords	Run a short campaign on passphrases, one password per account, and free password managers. Require two-factor authentication on student email and the portal. Screen new passwords against known breached lists and encourage a unique school password (Grassi et al., 2017).	University IT, student affairs	Within one semester
2 Everyday habits	Publish simple rules: avoid banking on public Wi-Fi, install apps only from official stores, switch off public location sharing, never send ID photos through chat apps, and check links and senders before acting on urgent messages. Make campus Wi-Fi secure and say so.	University IT, student affairs	Next orientation
3 Incidents and loan apps	Set up one clear reporting route (bank or fintech first, then the police cybercrime unit, then the university desk) and publicise it. Publish how to check whether a lender is registered with the FCCPC and how to complain. Collect anonymous incident figures each year.	Student affairs, legal unit, student union	Within one semester
4 Institution gap	Issue a plain-language student data notice saying what data the university holds, why, and for how long, and name a data protection contact. Add security to induction and make training visible.	Registrar, data protection officer, ICT	Within one academic year
5 AI deception	Add a short module on deepfakes and AI-written scams: verify requests through a second channel and a known number, never paste ID or bank details into chatbots, and treat voice or video alone as unproven.	ICT directorate, faculties	Next semester
6 Targeted training	Prioritise the four weakest topics (password reuse, padlock trust, public Wi-Fi, antivirus), delivered as live workshops and short videos, as students asked. Add consented phishing simulations with feedback (Kumaraguru et al., 2010), and measure before and after.	ICT directorate, student affairs	Phased over a year
All	Repeat the survey annually with respondent-level records, so that results can be broken down by level and field, and add a closer look at reporting behaviour.	Research unit, student affairs	Annual

Table 8. Problems, recommendations, suggested owners and timing.

For students. Pick one action this week: turn on two-factor authentication for your email, then give your school login a password you use nowhere else. Treat any message that combines urgency with authority as suspect and confirm it by calling a number you already know. Do not send ID photos through chat apps. Keep your phone's apps to the official store.

For researchers. The next step is to collect respondent-level data so that knowledge, practice and incidents can be linked, to test whether training changes behaviour over time, and to include other institutions. Comparisons across public and private universities would be especially useful.

8. Limitations

Several limits apply. The sample was reached by convenience and self-selected, and half of it came from one faculty, so results may not reflect the whole university (Etikan et al., 2016). Self-reports of behaviour may be flattering, and the common-method problem applies since every answer came from the same instrument (Nederhof, 1985; Podsakoff et al., 2003). The tallies were incomplete for many items, which is why percentages are lower bounds, and a few totals were inconsistent. I could not cross-tabulate or test

differences between groups, so statements about relationships between answers are inferences. Several items (E1 to E3, G4, H4, J2) could not be reported at all, which means the privacy-concern, reporting-awareness and AI-use pictures are partial, and the recommendations lack input from students' own open suggestions. The study measures stated knowledge and habits and not actual security outcomes. One institution at one moment cannot speak for all Nigerian universities, and the threat landscape changes quickly.

9. Conclusion

University of Lagos students know and do the things that have been drilled into them: they guard their OTPs, lock their phones and use two-factor authentication. They are far weaker on the less visible things, such as reusing passwords, trusting padlocks, banking on public Wi-Fi and sending ID photos to a chat. That gap shows up in a high rate of scams, harassment and money lost, and in a sense that newer, AI-enabled tricks are beyond them.

The encouraging part is the demand. Almost every respondent wants more training and most would report an incident if they knew where to go. The task for the university is to supply what students are asking for, aimed at the specific habits that put them at risk, and to make its own rules and reporting routes visible. The findings here describe what students say they know and do, and the next piece of evidence needed is whether better training actually changes what they do.

Declarations

Ethics. The study received an ethics exemption from the University of Lagos Research Ethics Committee (UNILAGREC), Informed consent was obtained from all participants on the first page of the online form before they could answer any question.

Sponsorship and independence. The research was sponsored by UGTF, Detroit, Michigan, USA (ugtf.org). The author is employed by UGTF as Lead Software Engineer. The sponsor had no role in the analysis or reporting of the results and did not have access to individual responses.

Data. Raw responses were kept only for the analysis period of about three weeks and are then deleted in line with the study protocol. Aggregate tallies are available from the author on request.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
- Channels TV. (2025). *FCCPC unveils rules to end loan app harassment, impose ₦100m sanctions*. Retrieved October 2026, from <https://www.channelstv.com/?p=955420>
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820.
- Cialdini, R. B. (2009). *Influence: Science and practice* (5th ed.). Pearson.
- Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). Wiley.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.
- Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.
- Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581-590.
- Dunning, D., & Kruger, J. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, 77(6), 1121-1134.
- Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873-2882.
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4.
- Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*.
- Grassi, P. A., Fenton, J. L., Newton, E. M., et al. (2017). *Digital identity guidelines: Authentication and lifecycle management* (NIST Special Publication 800-63B). National Institute of Standards and Technology.
- Ion, I., Reeder, R., & Consolvo, S. (2015). "...no one can hack my mind": Comparing expert and non-expert security practices. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 327-346.
- KPMG Nigeria. (2023). *The Nigeria Data Protection Act, 2023*. Retrieved October 2026, from <https://kpmg.com/ng/en/home/insights/2023/09/the-nigeria-data-protection-act--2023.html>
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), Article 7.
- Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, 22(140), 1-55.
- Nairametrics. (2023). *Loan apps defy FCCPC, as customer defamation and harassment continues*. Retrieved October 2026, from <https://nairametrics.com/?p=457794>
- Nederhof, A. J. (1985). Methods of coping with social desirability bias: A review. *European Journal of Social Psychology*, 15(3), 263-280.
- Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93-114.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.
- Verizon. (2024). *2024 Data Breach Investigations Report*. Verizon Business.
- Wash, R. (2010). Folk models of home computer security. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, Article 11.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE.

Appendix A. Questionnaire Items

Items C1 to C10 used true, false or not sure. Items D1 to D11, H3 and H4 used never, rarely, sometimes, often, always. Items E1 to E7, G3 to G5, H2 and I1 to I6 used strongly disagree to strongly agree. Other items used the response options shown in the survey form.

A1. I have read the information and agree to take part. A2. I am 18 or older and currently enrolled at the University of Lagos.

B1. Level of study. B2. Faculty or field. B3. Age group. B4. Gender. B5. Main device. B6. Main internet source. B7. Hours online per day. B8. Online services used regularly (select all).

C1. Using the same password on several accounts is safe if the password is long. C2. A padlock icon guarantees that a website is genuine and safe. C3. Public Wi-Fi can allow other people to see some of your online activity. C4. Two-factor authentication still protects an account even if the password is stolen. C5. A bank will never ask for your OTP or PIN over a call, SMS or chat. C6. Phishing attacks only happen through email. C7. Installing updates helps fix known security weaknesses. C8. Antivirus software alone protects you from all online threats. C9. A message saying your account will close in 24 hours unless you click a link should make you suspicious. C10. Apps downloaded outside official app stores carry a higher risk of malware.

D1. I use a different password for each important account. D2. My passwords are long (12 or more characters) or are passphrases. D3. I use two-factor authentication on my email and banking or fintech accounts. D4. I install updates soon after they appear. D5. I check the sender and the link before acting on an urgent message. D6. I use public Wi-Fi to log into banking or other important accounts. D7. I share an OTP, PIN or password with someone else. D8. I install apps from outside the official app store. D9. I back up important files. D10. I lock my phone or laptop with a PIN, password or fingerprint. D11. I use my school email or portal password on other websites.

E1. I am concerned about how apps and websites collect my personal data. E2. I regularly review the privacy settings on my social media accounts. E3. I read the permissions an app asks for before I accept them. E4. I often share my location publicly on social media. E5. I would send a photo of my ID card, BVN or NIN through a chat app if someone I trust asked. E6. I trust my institution to protect the personal data it holds about me. E7. I know what personal data my institution keeps about me. E8. I understand the Nigeria Data Protection Act 2023 and what rights it gives me.

F1. Which of these have happened to you in the last 12 months? (select all). F2. If you lost money, about how much in total? F3. Who did you report the incident to? F4. If you did not report, why? F5. Which threats worry you most? (choose up to 3).

G1. Where have you learned most of what you know about online safety? G2. Has your institution offered any cybersecurity training or orientation? G3. I know the institution has an IT or data-protection policy for students. G4. I know how to report a cyber incident at my institution. G5. The institution's systems feel secure to me. G6. Which training format would help you most?

H1. I have seen a deepfake or AI-generated fake of a real person's face or voice. H2. I can tell AI-written scam messages from genuine ones. H3. I type sensitive personal information into AI chatbots. H4. I use an AI tool to check whether a message or link is a scam.

I1. I feel confident that I can recognise a phishing message. I2. Online security is the IT department's job, not mine. I3. Security measures such as strong passwords and two-factor authentication are too inconvenient. I4. I believe I could become the target of an online scam. I5. I would like more training on staying safe online. I6. I would report a suspicious incident if I knew where to report it.

J1. What is the biggest cybersecurity problem students face at your institution? J2. What one thing should the institution do to help students stay safe online?