JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(3), 1770-1779
ISSN: 2589-1316

Cybersecurity and the Culture of Protection from Digital Danger: A Sociocultural Study of University Students in Saudi Arabia

Mohamed Ayari[1], Atef Gharbi[2], Nasser Albalawi[3], Zeineb Klai[4], Mahmoud Salaheldin Elsayed[5], Albia Maqbool[6]

[1] *Department of Information Technology, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, SAUDI ARABIA*
[2] *Department of Information Systems, Faculty of Computing and Information Technology, Northern Border University, Rafha 91911, SAUDI ARABIA*
[3,4,5,6] *Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha, SAUDI ARABIA*

*__Corresponding Author:__ Mohamed.ayari@nbu.edu.sa

Citation: Ayari, M., Gharbi, A., Albalawi, N., Klai, Z., Elsayed, M. S. & Maqbool, A. (2025). Cybersecurity and the Culture of Protection from Digital Danger: A Sociocultural Study of University Students in Saudi Arabia, *Journal of Cultural Analysis and Social Change*, 10(3), 1770-1779. https://doi.org/10.64753/jcasc.v10i3.2667

Published: December 02, 2025

ABSTRACT

Daily life for university students in Saudi Arabia is now closely bound up with social media, messaging apps and online learning platforms. This dependence exposes them to a range of digital threats such as account hacking, harassment and reputational damage. This article explores how students develop a shared "culture of protection" against these dangers in their everyday online practices. Using a sociocultural lens and drawing on an exploratory study with Saudi university students, it examines how family expectations, religious values, gender norms and peer relations shape what they see as risky, whom they trust and how they choose to protect themselves. The analysis highlights three key dynamics: the moral framing of online behaviour as a responsibility toward self and family; the constant balancing of openness and control when managing visibility on social media; and a strong reliance on informal networks—friends, siblings and classmates—rather than formal institutional channels for security support. The article argues that cybersecurity policies and awareness initiatives in higher education are more effective when they build on these lived cultural logics instead of treating students as isolated technical users.

Keywords: Cybersecurity; Digital Danger; Culture of Protection; University Students; Saudi Arabia; Sociocultural Analysis

INTRODUCTION

Young people's social, educational and economic lives are now structured by digital technologies to a greater extent than at any point before. Services as platforms—from learning management and cloud storage systems to social media and mobile payment apps—have ushered in an era of what is referred to as the 'platform society' (van Dijcket al. 2018). These infrastructures are not extraneous tools for university students, they are the primary site in which they will study, socialise, organise themselves and imagine their future. And in this sense, questions of cybersecurity are never just technical ones: they rest fundamentally on how young people come to understand trust, responsibility and risk in their digital lives.

International dialogues about young people in the digital age have moved beyond a narrow understanding of online risks to embrace a more rich and nuanced picture of digital resilience, wellbeing and agency. Recent work highlights protective practices as arising from complex negotiations among young people, families, schools and platforms rather than individual skills in isolation. Studies of digital resilience find protective factors to be not just

technical, but also peer norms, family communication styles and larger cultural expectations regarding risk, shame and reputation. Research on young people's notions of digital privacy suggests they see privacy as a right and as something for which they are individually responsible, the concept being one that can be likened to their "digital safety" alongside an ability to engage online without risk of misuse (or identity or data) and misconstruction (Vespoli et al. 2024; Walrave et al. 2024). These observations tell us that we need to adopt sociocultural framings like this, which regard cybersecurity practices as part of the broader cultural landscape in which young people live with digital technologies.

A sociocultural lens is especially apt for what we call culture of protection from digital harm: the mutually understood meanings, norms and quotidian practices through which individuals understand digital risks and decide how, if at all, to protect themselves and others. This is consistent with, and reflects new developments on "cybersecurity culture", which already frames security-centred beliefs, values and practices as embedded in organisational and societal culture than reducible to individual awareness (ENISA 2017; Uchendu et al. 2021). Cybersecurity policy constructs like the Cybersecurity Capacity Maturity Model for Nations (CCMMN) also recognize "cybersecurity culture and society" as a fundamental dimension of national capacity, emphasizing the role of trust, social norms, and public attitudes among technical controls in mitigating cyber threats (Global Cyber Security Capacity Centre 2021). Saudi Arabia's national programs, such as the Saudi Cybersecurity Higher Education, Research and Innovation Framework (SCyber-Edu), also emphasise culture and education as strategic enablers to build resilience (National Cybersecurity Authority 2024). These views suggest that to understand how young people learn to keep safe in digital environments we cannot ignore the impact of social relationships, institutional contexts and cultural narratives, and not just knowledge about passwords and malware.

Education institutions among the key spaces where these cultures of protection are enacted and fought over. University students are intensive and comparatively unsupervised users of networked technologies, typically juggling multiple identities between learning platforms, messaging apps and public social media. As is true in studies of students beyond Saudi Arabia, large-scale survey results have revealed that although many students are equipped with rudimentary knowledge of cybersecurity practices, they feel woefully unprepared in such areas as password management, phishing recognition, and incident reporting (Alharbi and Tassaddiq 2021; Aljohni et al. 2021; Alzubaidi 2021). Such research has emphasized a continuing "knowing–doing gap": that students know about recommended practices but do not carry through with behaviour change over time (47). This divergence has helped drive the calls for a more strategic focus on security that moves away from reactive provision of ad hoc awareness programs toward strategies that interweave cybersecurity into the scholarly culture and daily routines (Ivanova and Bogdanova 2025).

Yet at the same time, Saudi Arabia has experienced a massive digital transformation and has among the highest rates of social media use in the world, particularly for young people. Studies on Saudi youth and young people reveal that social media networks have become vital sites for identity experimentation, gendered negotiations, and national belonging. Representative studies of the construction of identity among Saudi adolescents show how young users cope with global, on line cultures and local religious and cultural norms through Natasa Lackovic: Digital anthropology in the age of big data 25 social networking media by experimenting with new ways to fashion a self-presentation, while also managing family and community expectations (Muyidi 2025; Almahmoud et al. 2025). Other research studies how Saudi young people behave on social media in conditions of extreme social visibility, where one misstep can damage the reputation of an individual and their family (Stanger et al. 2017; Hammad 2022). These dynamics mean that digital danger for Saudi youth is not here just technological attacks, but also moral, reputational and relational risks.

These are important works, but there is still a gap in the literature as it pertains to sociocultural studies of youth in Saudi Arabia and cyber security research. The majority of literature on cybersecurity tends to quantify awareness and suggest training, but does little in the way to how students themselves understand what constitutes digital danger, who they hold accountable for their safety online, or how their practices are influenced by gendered dynamics, choice of study subject, familial expectations or narratives of national security (Alharbi and Tassaddiq 2021; Aljohni et al. 2021; Ivanova and Bogdanova 2025). Second, research on Saudi youth's social media practices and identity construction seldom centered cybersecurity and digital safety as key analytic elements (Muyidi 2025; Almahmoud et al. 2025; Stanger et al. 2017). At the international level, there have been calls from conceptual and policy work for context-sensitive, participatory cybersecurity cultures (ENISA 2017; Global Cyber Security Capacity Centre 2021; Ivanova and Bogdanova 2025) however qualitative research that investigates such cultures among university students in non-Western countries is still rather limited.

To fill such gaps, this paper builds on a sociocultural investigation into cybersecurity and the culture of protection against digital threats among university students in Saudi Arabia. The emphasis is not on student victims or bits of flotsam drifting in the increasingly treacherous edtech stream, but on active interpreters of digital risk who employ cultural capital, peer norms, and institutional messaging to decide what to do online (Cortesi et al. The research question is: How do Saudi university students perceive digital risk and cyber safety in their daily

life? What are the shared norms, stories and practices that make up their culture of protection against digital harm? What is the influence of sex, subject area and broader social and national discourses on these cultures? What do these results mean with respect to developing culturally relevant and authentic cybersecurity education and policy for students?

By bringing out students' accounts themselves, the study also adds a new and richer layer of understanding to survey-based assessments of cybersecurity awareness: that protectively-oriented practices are apparently learnt, negotiated with and sometimes rejected within a particular socio-cultural setting. It also connects the empirical context to wider discussions about digital citizenship and youth resilience, framing cyber security as not just following technical specifications but as part of how young people understand safe and respectful engagement in digital life (UNICEF Office of Research–Innocenti 2024; Phippen and Street 2021; Oguine et al. 2025; Hassoun et al. 2024). Knowledge of the culture of protection from digital danger among Saudi University students is necessary to inform a national approach which aims to integrate cybersecurity into higher education and everyday practice (National Cybersecurity Authority 2024).

The remainder of the paper is structured as follows: Section 2 presents a review of literature relating to cybersecurity culture, youth digital practices and the context of Saudi higher education. Method In the following Section 3, we present both our methodological approach and data collection methods. In Section 4, we describe the students' understandings and practice concerning protection against digital dangers through an empirical analysis. We conclude with a summary of the implications of these results for cybersecurity education, policy, and future research in Section 5. Section 6 concludes the paper.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

Cybersecurity is frequently framed as a technical challenge to be overcome in the securing of networks, devices and data, but ordinary instances of security and insecurity are profoundly social and cultural. In the platform society, where central social practices, such as communication, education and labouring, but also media consumption is intermediated through big digital platforms, security questions become entangled in how values – value - is negotiated between public and private online. For college students who conduct so much of their social and academic lives through these platforms, cybersecurity becomes just another way to govern identity, relationships and safety. This section locates the study within a series of overlapping areas of scholarship: culture and society in cybersecurity, youth doing with digital technologies, risk and resilience, Cybersecurity and higher education, and the particular context of Saudi Arabia's becoming digitally transformed.

Research on cybersecurity culture has expanded from a purely technical view of security to a more broad understanding including shared beliefs, values and norms. Instead of looking at security as "items" and behaviours, this literature is more interested in informal practices, mutual influence and sense-making around what constitutes reasonable or normal security – both within organizations and society at large. At national level, frameworks like the Cybersecurity Capacity Maturity Model for Nations include cybersecurity culture and society as central dimensions of capacity, and highlight components like public risk attitudes, institutional trust levels and media depictions of cyber risks. Culture and education in Saudi policy in a similar vein, culture and education are placed as strategic pillars in Saudi policy to build resilience.

Studies of young people's digital practices and digital resilience have shown that youth are not simply victims of online risk, but rather active agents who engage in strategic responses to digitally meditated threats by managing these risks, avoiding them or resisting them. Protective factors include digital literacies, social support, positive school climates and filtering of information on the internet. Simultaneously, research on teenagers' perceptions of privacy and safety online show that these are constructed as both rights and relational orderings bound up with friendship networks, family expectations, and worries about being tainted by their reputations. This work contributes to a move away from protectionists discourses towards those that foreground empowerment, participation and resilience.

In higher education, universities are key locations of cybersecurity activity due to their role as keepers of sensitive data and providers of the next generation's computing workforce and citizenry. A wide range of research papers evaluate the computer and network security awareness among university students; these studies report that both knowledgeی' levels are moderate, as well as highlights on-going disconnect with good password handling, detecting phishing attacks and incident reporting. These results highlight a "knowing–doing gap" and the imperative to integrate cybersecurity as an aspect of an institution's culture, curricula, and pedagogical practices rather than just repeating one-time awareness-raising campaigns.

Saudi Arabia offers a particularly interesting context for investigating the cultural attitudes towards and perceptions of protection against digital harm. The country is a young one, with high rates of social media usage, and online platforms are important places for socialization, experimenting with self-presentation and exchange between local and global cultures. One thing studies have begun to reveal is the manner in which Saudi young play

off media globalization with local religious and cultural standards, engaging social media both as means for discovering new forms of self-expression and a tool to keep up family and community expectations. Social media is also implicated in building and reinforcing national identity, while simultaneously exposing students to new forms of visibility and comparison within the social. These dynamics suggest that digital risk is not just a technical danger but also a moral, reputational and relational one.

From these threads, the study frames a culture of protection from digital danger as the constellation of shared meanings, norms and taken for granted practices through which a group makes sense of what constitutes digital threat and how to respond. This culture consists of a sensibility toward risk, moral and relational logics, practical routines, and knowledge-based authorities. Inspired by cybersecurity culture frameworks, it is however contextualized in the everyday lives of Saudi university students as depicted in youth digital practices and identities research. By approaching students as cultural actors in their own right, rather than passive recipients of awareness campaigns, the analysis considers how they work through competing concerns—safety versus sociability; autonomy and independence versus familial expectations; convenience against caution—in enacting their own quotidian cartographies of protection.

METHODOLOGY

Research Design

The framework is largely exploratory and interpretive. Unlike a conventional hypothesis-testing study the investigation is not designed to test some predetermined set of hypotheses but rather to describe and explain the culture of protection against digital danger as it is enacted in students' day-today university and online lives. A mixed-method approach was used to:

- Describe general trends in awareness, perceived susceptibility and reported behavior among a wider range of students;
- Document rich stories about family, religion, gender, and peer relationships that shape digital practices;
- Compare what students say they do, in responses to surveys, with how they talk about their decisions and dilemmas in more open conversational settings.

Both strands of data are assumed to complement each other. The quantitative data from the questionnaire are utilized in order to situate and compare qualitative themes, while the interview and focus group data are employed to help make sense of unexpected or diverging patterns from the survey.

Setting and Participants

The sample was recruited from participants were undergraduate students at a public university in Saudi Arabia, plus those from one other neighboring institution to broaden viewpoints. These universities were chosen as they have strong digital learning environments and student engagement with social media and online spaces.

Participants were advertised through posts on university learning management systems, university email and student WhatsApp and Telegram groups. Students had to be enrolled in undergraduate study programmes with regular access to the internet and social media. All attempts were made for gender, academic discipline (e.g., computer science and IT, engineering, education; social sciences and business) and years of study distribution.

In the end, some 200 respondents decided to answer the questionnaire online. From these, a prepared to participate in interviews and focus groups. Since we aimed to ensure a variation in gender, fields of study and the level of reported cyber-security awareness and concern (as derived from the responses in the questionnaire) – we strived for diversity in these attributes when selecting the participants for our qualitative phase.

Data Collection

Questionnaire

The survey was provided to participants via an online survey site. It included four main parts:

1. ***Demographic and Educational Background***
   Age, gender, academic programme and year of study and average daily hours online;
2. ***Digital Practices and Device Use***
   For types of devices, main online activities (e.g., learning platforms, social media, gaming, purchasing goods or services), and contexts of use (i.e. home, on campus or in public Wi-Fi spaces);
3. ***Attitudes toward Digital Risks and Cybersecurity***

Levels of threat severity (probabilities of occurrence) and risk seriousness for various threats, represented in a questionnaire featuring risks including password compromise, account hacking, online harassment, harm to reputation, data privacy abuse and financial fraud;

4. ***Protective Practices and Responses***

Self-reported password use, privacy settings, verifying links and messages, reporting things that seem suspicious to a moderator or Redditor admin), self-reported security awareness (e.g.

The majority of items were in a Likert response format and measure agreement or frequency of behaviours, while open-ended questions asked students to describe the most serious "digital danger" they had experienced or witnessed and what action they took.

Development of questionnaire The questionnaire was originally written in English, and translated into Arabic by Bilingual speaking colleagues for clarity and culture. A small pilot with students was conducted to verify wording and length; slight verbiage changes were made prior to dissemination.

Interviews and Focus Groups

Semi-structured interviews and focus groups were then employed to delve further into how pupils understand digital danger and protection. An interview guide and synthesis of key issues.

1. Experiences of being safe or unsafe online;
2. Stories about friends, family, or schoolmates who had a close call;
3. Knowledge and advice on cyber-security sources (family, peers, formal education staff, online materials, official campaigns);
4. Whether cultural and religious values affects what they feel is OK or not safe to do online;
5. Trade-offs between being connected, visible on social media and protecting privacy and reputation.

Interviews were carried out individually because some students expressed a desire to have one-one discussions, while focus-groups enabled small groups of four to six persons who felt comfortable discussing their experiences in company. Both formats were conducted in the language selected by participants (Arabic, English or a combination) and audio recorded with permission. Sessions generally ranged from forty-five to sixty minutes.

Data Analysis

Descriptive analysis was conducted using statistical package on the questionnaire information. For brevity, cross-tabulations and frequencies are used to assess general trends in perceived risks and protective behaviours by sex, discipline, and year of study. These descriptive statistics served as background for a qualitative interpretation, but not the ultimate study outcome.

Transcripts were made of interview and focus group recordings, which if required were translated into English using the services of a professional translator for analysis. Thematic analysis was carried out in several stages:

1. ***Immersion***—reading and re-reading transcripts to get a foothold on the participants' narratives;
2. ***Initial Coding*** –; the relevance of text to perceptions of digital threats, protective actions, feeling vulnerable or safe and references to family and religion, either creating anxiety or security.
3. ***Creating Themes*** – clustering codes according to overarching themes such as "name protection," "trusted inner circle," "gendered visibility expectations" or "learning from events";
4. ***Further Refining and Relating of Themes*** – examining the ways in which themes related to each other in the identification process, as well as how they related to issues or patterns in the questionnaire-based data (including through similarity, difference, multiplication effect), and according to gender, discipline and levels of self-reported awareness.

The analysis strove to maintain students' own language and categories as well as a develop more abstract conceptualizations that capture common cultural logics of protection from digital danger.

Ethical Considerations

The study was approved by the local institutional review body (ethics approval). Voluntary participation under informed consent was applied. The information sheet described the purpose of the study, what participation entailed, possible risks and benefits to participant involvement and steps taken to ensure confidentiality.

For the questionnaire, no personal information was asked except for basic demographic data and answers were kept anonymous. Pseudonyms were applied to all participants in transcripts and any identifying information was omitted or changed for interviews or focus group. Participants were instructed that they could refuse to answer any questions or withdraw from the study at any time without consequence.

Sensitive situations, such as cases of harassment, blackmail or reputation damage were discussed with special precautions. The participants were asked not to reveal names or specifics of the individuals that could cause others to be identified, and a sheet with contact details for nearby support services was distributed in order to deal with any anxieties provoked by discussions.

Methodological Reflections

The proposed system has some advantages. [28] An added benefit of a survey complemented by interviews and focus groups is that it enables the researcher to see patterns in broader social meanings as well as meaning making within context. Studying more than one university enhances the multiple lens of looking on while at the same time not precluding attention to singularity of the Saudi higher education circumstance. Interviews and focus groups in students' language of preference facilitate a more genuine and nuanced narrative.

At the same time, there are limits to the study. The participations were voluntary and also convenience samples participation, which might imply that those students already will be interested or have some concern about digital related issues. Social desirability bias, however, is inherent in the self-reporting of behaviour to questionnaires and particularly on issues concerning responsibility and adherence. The qualitative sample, while extremely detailed, may not be generalizable to all Saudi university students.

These limitations notwithstanding, the method was well suited to the exploratory nature of our investigation: to uncover how cybersecurity is embedded within students' everyday lives as part of a wider culture of protecting oneself against digital threats.

RESULTS: CULTURES OF PROTECTION FROM DIGITAL DANGER

Results: Cultures of Protection in the Age of Digital Risk

The findings of the empirical material show that cybersecurity, for these students, is not perceived as a collection of isolated technical rules. Instead, it reads like a weaving of anxieties for faith, family honor, friendship, gender-based expectation and academic success. When students spoke about the "digital danger," they seamlessly transitioned between anecdotes of hacked accounts, embarrassing screenshots and gossip spreading through family WhatsApp groups.

The findings that follow are structured around five interlinked dimensions:

(i) Students' definitions of digital danger.
(ii) Moral responsibility and the family.
(iii) Managing visibility and gendered norms.
(iv) Everyday protective practices and informal expertise and (v)tensions and contradictions within their culture of protection.

Digital Danger as Technical, Moral and Social Risk

He then asked them to describe what "digital danger" looks like, though with that race in the back of his mind as he read. Instead, they began with real stories: a cousin whose Snapchat account was hacked and sent offensive messages, a classmate who right before exams found the password to her email account changed, a friend whose edited photo made it onto Instagram without permission.

From the survey and qualitative data, three types of digital danger fell into broad categories:

1. ***Technological Compromise*** – not having control on the accounts or devices, example hacking, phishing and Spyware application.
2. ***Reputational Harm*** – screenshots, rumours, or doctored images that could damage the reputation of the individual or their family.
3. ***Emotional and Relational Damage*** – harassment, extortion or abuse of trust in online relations.

Technical dangers were often characterized as such because of the impact they had on the other two classes. That is a hacked account was distressing not so much for its methodological provenance as for its ability to send inappropriate material, leak private conversations or disgrace parents and siblings. In this way, digital threat was for many participants characterized by its "escaping control" and circulating beyond the target.

Students also related digital risk to time and speed. Some suggested that online problems can "grow fast" and "spread in minutes," making it hard to contain harm. This notion of acceleration heightened relevance of anticipation and prudence over reaction.

Moral Responsibility and the Household

Conversations about cybersecurity rapidly became conversations about accountability. A number of students positioned their online activities as part of a broader moral commitment to the family. Sibling: The character, like a sibling would in the offline world, asks if they can maintain three accounts instead of two and then work as a 'slave' for them to repay their kindness. These entreaties fall under questions about forwarding 'rumours', or consuming 'dirty' content where saying no to these requests is also seen as defending the "name of the family".

The students articulated a nuanced perception of responsibility:

- Responsibility to Myself – the safeguarding of one's personal data, future career and integrity.

- Duty to Family – stay out of trouble, avoid any scandal or bringing shame or worry.
- Duty to Others – Don't get friends or classmates sick with careless sharing and gossip.

For many, that moral dimension made cybersecurity not simply a technical necessity but a question of character. Some people I spoke with thought that goofing off online is a sign of immaturity or disrespect, especially if it puts other people at risk. Students also varied in the extent to which they engaged their families on digital matters. Some children sought support from parents, or older siblings, in response to suspecting messages or apps but some preferred to deal with that kind of issue on their own because they worried that parental controls might be introduced or things could get misinterpreted.

Visibility: Gender, Platforms and Boundaries

Gender was a big part of the equation for how students were processing visibility and protection. For many women in the study, that meant careful strategies for who got access to their photos, posts and contact information. Some such tactics involved creating private accounts, keeping followers small and not using a profile picture that showed their face — or even managing separate "public" and "close friends" profiles.

Some male students also mentioned concerns about visibility (especially worrying about future employment, or mandatory military or security background checks), but overall anxiety regarding photos and reputational gossip was higher among women. Some students, regardless of their gender, said an image or voice note could come back to "follow you for eternity," especially in close-knit communities.

The platform decision was itself a matter of protection culture. Students thought that different uses came with different risks. For example:

- WhatsApp and Telegram were often considered relatively "safe" for family- and study-related groups but dangerous for larger or unfamiliar groups.
- Snapchat was perceived as more casual and "ephemeral," yet students were very aware that screenshots could be captured and preserved.
- Instagram, X and TikTok were treated as public squares where posts can spread well beyond the intended audience.

A lot of students adapted their behaviour, restricting the most personal content to intimate groups but using public platforms for more neutral or professional content. This careful division of audiences is part of their culture of protecting themselves from digital danger.

The Informant and Quotidian Protective Practices

The responses to the questionnaire indicated that in general, students were aware of basic security hygiene measures such as using unique passwords and turning on two factor authentication or recognizing if a phishing message was too obvious. Nevertheless, qualitative discussions indicated these practices were not universally implemented. While some students always followed the advice, others knew what to do but reused passwords and dismissed security warnings when feeling rushed or tired.

Students reported a variety of protective behaviors that they performed on a daily basis, including:

investigating the source of a spontaneous link prior to clicking on it;

- checking things out with a friend or family member if any message that seems to be sent by them, appears "odd";
- having study and private e-mail accounts, but then using a third account for online shopping;
- not sharing location information in real time;
- regularly checking privacy settings when an app updates.

Non-formal knowledge networks were central in disseminating these practices. Many students reported initially turning to friends or classmates — and, less often, adults in the school community — when they received troubling messages or were unfamiliar with security features. Amongst friendship groups, some people eventually became known as "the security guy." These unofficial experts can help someone set a device, recover an account or understand new security features in a way that mere official instructions somehow cannot.

This dependence on informal expertise comes with its strengths and vulnerabilities. For one thing, advice from trusted colleagues can be more convincing and linguistically comprehensible than formal training. On the other hand, if that "expert" has wrong or outdated information, bad practices can be just as contagious.

Table 1 Overview of key categories in students' culture of protection

Table 1: Main dimensions of the culture of protection from digital danger for students

Dimension	Brief description
Perceptions of digital danger	Threats in this context shall mean a convergence of technologically based threat, reputational-based threat and emotional-relational based threats.
Moral responsibility	Online conduct as care of self, family and others; protection as quality of character.

	.
Managing visibility	Concerted management of photos, writing and audience—gendered norms constitute how something is either risky or safe to discuss.
Everyday protective practices	Suggestions and hacks, using a mix of recommended measures (passwords, privacy controls) and DIY techniques suited to different online platforms and situations.
Informal expertise	Peers, siblings and classmates often fill the role of advisors; some became "local experts" in cyber security.
Tensions and contradictions	Divides between knowledge and action, safety and sociability, trust and suspicion in online encounters.

Tensions and Contradictions

Underneath the protective culture of sharing, however, students' narratives pointed instead to a collection of ongoing, everyday relationships and tensions. Three tensions were particularly prominent.

First is the tension between theory and practice. Many of the people were able to articulate safe practices in abstract but also admitted that they don't always perform them — especially not when speed and convenience are factors. For instance, a student could know that unique passwords are important but recycle one or two across multiple platforms because they "can't keep track of all of them."

Second, students felt conflict between safety and sociability. Some defensive moves, like setting accounts to private or not following back or restricting interactions with mixed-gender groups, were perceived as socially expensive. Students worried that they would be seen as unfriendly, too cautious or "paranoid." Therefore, they typically struck a compromise at some balance point, taking on so many risks needing to maintain relations or prevent misunderstandings.

A third was the tension between trust and suspicion. On the other hand, the students highlighted how trusting in close friends and family is very important. On the other, they knew that much digital harm originates in these intimate spaces, through shared devices, guessed passwords or forwarded screenshots. This ambivalence was most evident in the context of sharing devices or accounts across families and friends.

These tensions are not evidence that cybersecurity education is failing; instead, they show that students are negotiating complex decisions in the midst of thickets of social and cultural beliefs. Indeed, the ethos of protection against digital harm discerned in this study is better described as a negotiated and to some extent precarious peace than a set of necessary immutable laws.

DISCUSSION

The results demonstrate that cybersecurity is experienced as a moral and relational activity for Saudi university students, rather than as a technical to do list. Digital perils aren't restricted to malware or hackers; they include the threat of reputation damage, lost trust, and embarrassment for you and your family. Safeguarding accounts, hardware and info is hence also the same as safeguarding your dignity, honour and any future chances you might have.

Students' tactics of care are influenced by norms around gender and platform cultures. Some women explained elaborate strategies for controlling who sees their posts — via second accounts, selective sharing and careful image management — that take them beyond typical security advice. These are not only performances of fear; they are deliberate, thoughtful strategies for mediating between the dictates of self-expression and social or religious regulation. Male students, although typically less restricted by images, also had concerns about the long-term impact for their careers and reputations.

The research also brings out a sharp tension between what students know and what they actually do. Many respondents can recite best practices — strong, unique passwords; multi-factor authentication — yet confess that they do not always adhere to these guidelines. There are shortcuts, of course, because when you're tired and want to avoid being that rigorous friend, these things tend to happen. Going out — rather than being constituted solely as negligence, the willful flouting of evident risks — was a matter of negotiation: students were making calculations and trade-offs between safety and sociability, trust and suspicion, caution and paranoia or unfriendliness.

Critically, informal networks of experts are also central to the culture of secrecy. Students have always, to a great extent depended on good friends, siblings and we the juniors or seniors for guidance, proposed solution of problems or what should be your response in situations. In many of these local experts are successful, where formal campaigns fail, because they translate things in to familiar language, show settings on device directly and embedded within same social worlds. But this dependence can also mean that holes or errors in one subgroup may be replicated and magnified.

In sum, we argue that attempts to build cybersecurity knowledge and awareness among university students will be more successful if they can augment existing cultural logics of care and responsibility — rather than treating

students as isolated end users. Awareness campaigns that promote values such as family honour, assistance to friends, and good online citizenship are probably more effective than purely technical "input here" guidance. Engaging students in the co-design of standards, peer education programmes and reporting mechanisms may also help to close this gap between policy and practice.

CONCLUSION

This research aimed to explore how creating a culture of protection from digital danger in everyday life occurs among Saudi university students. Instead of perceiving 'the cyber' as either a purely technical or an awareness problem, the results show how meanings are woven together in a thick web, where technical risks can hardly be distinguished from moral, relational or reputational risks.

The analysis demonstrates that students' risk mitigation is informed by three principal dynamics: moral obligation, visibility management and use of informal expert networks. Indeed, students often regard online behaviour as part and parcel of what it means to be a good son or daughter, friend and citizen within the digital sphere and have received advice from peers, siblings or older students rather than any formal institutional mechanism when dealing with threats online.

These dynamics create several areas of tension. DM Students tend to know what safe practice looks like however do not always behave safely, particularly when convenience or social norms conflict. What motivates them is safety, but they don't want to seem paranoid or unresponsive. They have faith in close contacts, while knowing many cases originate within those circles.

For universities and policy makers, the findings hold a warning: any effective cybersecurity strategy must attend seriously to the cultural logics through which students make sense of digital danger. Efforts and campaigns that link technical advice to values of care, responsibility and mutual protection are more likely to get through than generic scare-mongering. Working with informal rather than against it—and including students in the actual design of programmes and means of recourse—goes much further to connect policy chess moves with life.

If we listen carefully to how students articulate their experiences and decisions, then you can start to recognize cybersecurity not just as a safeguarding of systems but as an integral part of the way in which young people strive to live safe, dignified and connected lives in a digitized world.

REFERENCES

Alharbi, T. and Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23.

Aljohni, W., Elfadil, N., Jarajreh, M. and Gasmelsied, M. (2021). Cybersecurity awareness level: The case of Saudi Arabia university students. International Journal of Advanced Computer Science and Applications, 12(3).

Almahmoud, M., Swanson, D. P., Luehmann, A., Duckles, J. and Whitesell, C. (2025). Saudi adolescents' identity development and social media use: An exploratory study. In M. M. Rahman, et al. (eds), Handbook of families in the Arab Gulf States (pp. 323–339). Cham: Springer.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(3), e06016.

ENISA (European Union Agency for Network and Information Security). (2017). Cybersecurity culture in organisations. Athens: ENISA.

Global Cyber Security Capacity Centre. (2021). Cybersecurity capacity maturity model for nations (CMM): Dimension 2 – Cybersecurity culture and society (2021 ed.). Oxford: University of Oxford.

Hammad, M. (2022). Social media and its impact on promoting the national identity of university students in Saudi Arabia. Journal of Social Sciences and Education, 4(1), 45–63.

Hassoun, N., Rizzi, M., Zannoni, M. and Bryanton, K. (2024). Shifting from protection to empowerment: Resilience-based perspectives on children and youths' online experiences. Social Sciences, 13(5).

Ivanova, G. and Bogdanova, G. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. Information, 16(5), 336.

Muyidi, A. (2025). Exploring how social media usage shapes self-presentation strategies among Saudi young adults. Frontiers in Psychology, 16, 1562917.

National Cybersecurity Authority. (2024). Saudi cybersecurity higher education, research and innovation framework (SCyber-Edu). Riyadh: National Cybersecurity Authority.

Oguine, O. C., et al. (2025). Online safety for all: Sociocultural insights from a systematic review. In Proceedings of the ACM Conference on Human Factors in Computing Systems. New York: ACM.

Phippen, A. and Street, R. (2021). Online resilience and wellbeing in young people: Public policy and digital safety. Cham: Palgrave Macmillan.

Stanger, N., Alnaghaimshi, N. and Pearson, E. (2017). How do Saudi youth engage with social media? First Monday, 22(5).

UNICEF Office of Research – Innocenti. (2024). Protecting young digital citizens in the digital age. Florence: UNICEF Office of Research – Innocenti.

Uchendu, B., Nurse, J. R. C., Bada, M. and Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.

Vespoli, G., Taddei, B., Imbimbo, E., De Luca, L. and Nocentini, A. (2024). The concept of privacy in the digital world according to teenagers. Journal of Public Health.

Walrave, M., Vangeel, J., De Wolf, R., et al. (2024). Protective factors contributing to adolescents' multifaceted digital resilience: A systematic literature review. Computers in Human Behavior.

van Dijck, J., Poell, T. and de Waal, M. (2018). The platform society: Public values in a connective world. Oxford: Oxford University Press.

