

DIGITALLY CONFIDENT BUT STILL VULNERABLE? CAPABILITY, ENGAGEMENT, AND PERCEIVED ONLINE SAFETY AMONG WOMEN IN NAIROBI, KENYA

Dr. Gideon Kirui.
Kenyatta University, Kenya.

©2026

International Academic Journal of Arts and Humanities (IAJAH) | ISSN 2520-4688

Received: 23rd September 2026

Published: 5th October 2026

Full Length Research

Available Online at: https://iajournals.org/articles/iajah_v2_i2_184_202.pdf

Citation: Kirui, G. (2026). Digitally confident but still vulnerable? Capability, engagement, and perceived online safety among women in Nairobi, Kenya. *International Academic Journal of Arts and Humanities*, 2(2), 184-202.

ABSTRACT

Women's digital participation provides opportunities for communication, learning and employment, but it also presents online safety risks. This study examined the relationships among digital confidence, formal digital safety training, internet use and perceived online safety among 208 adult women in Nairobi City County, Kenya. A cross-sectional survey was conducted using an online questionnaire, and the data were analysed using descriptive and multivariable statistical methods. The findings show that 58.2% of participants reported high or very high digital confidence, while 23.1% felt safe or very safe online. Formal digital safety training was associated with high or very high confidence (OR = 2.69, 95% CI [1.32, 5.49]), but was not independently associated with perceived online safety. Greater digital confidence was associated with higher

perceived safety (OR = 1.89, 95% CI [1.41, 2.54]), while more frequent internet use was associated with lower perceived safety (OR = 0.55, 95% CI [0.36, 0.83]). The findings indicate that perceived digital capability and perceived online safety are related but distinct. They suggest that digital safety interventions should develop individual capabilities alongside technological and institutional measures that support safer participation.

Keywords: Digital Confidence; Digital Safety Training; Perceived Online Safety; Technology-Facilitated Gender-Based Violence (TFGBV); Women's Digital Participation; Nairobi, Kenya

INTRODUCTION

Digital technologies are increasingly providing opportunities for communication, education, employment and public participation. However, their growing use also exposes women to risks—such as sexual harassment, cyberstalking, surveillance, gender trolling, sextortion and image-based abuse—all of which constitute forms of technology-facilitated gender-based violence (TFGBV) (UN Women, 2025). These challenges are particularly significant in low- and middle-income countries, where expanding digital access creates opportunities for empowerment while introducing additional risks (Tyabashe-Phume et al., 2025).

In response to these challenges, efforts to promote digital safety have increasingly emphasised digital skills, user confidence and protection against online abuse. Digital confidence reflects individuals' beliefs in their ability to navigate digital environments, while perceived online safety concerns their subjective sense of security when using digital technologies (Ulfert-Blank &

Schmidt, 2022). Although formal digital safety training may strengthen confidence and protective competencies (Khan et al., 2023), increased digital capability does not guarantee online safety (Livingstone et al., 2023). Evidence from Kenya indicates that online violence against women remains widespread, with low reporting rates among survivors (United Nations Population Fund [UNFPA], 2024, 2025).

Despite growing recognition of digital safety as essential to women's meaningful digital participation, limited empirical evidence exists on the relationships among digital safety training, digital confidence, internet-use frequency, and perceived online safety among adult women in sub-Saharan Africa. This study examined these relationships among adult women in Nairobi City County, Kenya. It considered previous TFGBV experience and selected socio-demographic characteristics. The findings provide evidence to inform digital safety interventions that address both individual capabilities and the broader conditions necessary for safe participation of women in digital environments.

LITERATURE REVIEW AND RESEARCH CONTEXT

Research has documented women's exposure to digital violence, but their perceived ability to protect themselves online has received less attention. Self-efficacy theory explains how beliefs about personal capability influence the ways individuals approach and manage particular situations (Bandura, 1997). In digital settings, confidence concerns perceived capability to recognise risks and apply protective measures, rather than access or technical competence alone (Ulfert-Blank & Schmidt, 2022). Digital literacy covers a broader set of competencies for accessing, evaluating and using digital information (Liu et al., 2026), including capabilities beyond technical proficiency (Afifah et al., 2026). Evidence from Uganda associates digital literacy with more favourable attitudes towards digital technology use among women (Abima et al., 2021). However, greater capability can expand opportunities without consistently reducing risk exposure (Livingstone et al., 2023). Information-navigation and communication skills have been associated with lower exposure. In contrast, technical and content-production skills can accompany greater exposure (Ambahelagedara et al., 2026). Although much of this research concerns younger populations, it provides a reason to examine capability and safety separately.

Digital confidence and perceived online safety concern different aspects of women's digital experiences. A woman may feel able to use privacy features and respond to threats while considering the wider online environment unsafe. Research on online risk management distinguishes digital skills, perceived control over risks and perceptions of risk (Helsper et al., 2025). Platform design, content moderation, other users' conduct and institutional responses also influence online safety. Research on violence against women identifies weaknesses in platform governance and regulation as relevant concerns (Pavón Pérez et al., 2026). Digital technologies can facilitate stalking, monitoring and harassment that require responses beyond technical competence (Henry et al., 2020). Within the Women, Peace and Security agenda, they can also

support participation while enabling gendered attacks (Baekgaard, 2024). Individual capability may help women manage particular threats without changing the conditions that permit those threats.

Studies of women in public-facing roles illustrate the consequences of online insecurity. A systematic review of 48 studies examining TFGBV against politically active women reported psychological distress, anxiety or fear in 81% of the studies; furthermore, changes in political messaging appeared in 62% and reduced online engagement in 39% (Koch et al., 2026). Journalists, activists and human rights defenders also experience digitally facilitated harassment and intimidation (Jankowicz et al., 2024). Among women journalists in Uganda, harassment can lead to changes in, or withdrawal from, online participation (Walulya & Selnes, 2023). These groups do not represent all women, but the findings demonstrate the relevance of online safety to overall well-being and democratic participation.

Formal digital safety training offers a practical approach to developing protective capability. Cybersecurity awareness training has been shown to improve self-efficacy and knowledge of threats and protective measures (Khan et al., 2023). Security self-efficacy, computer skills and previous experience have also been associated with protective cybersecurity behaviour (Anwar et al., 2017). Research involving women journalists in Uganda identifies training as relevant to confidence and resilience in responding to threats (Kakooza & Kazibwe, 2025). These findings accord with self-efficacy theory, which links skill acquisition and practice to confidence in performing particular actions (Bandura, 1997). Training may consequently have a closer relationship with digital confidence than with perceived online safety, since perceptions of safety also depend on conditions outside individual control.

Internet-use frequency introduces another consideration. Repeated use provides opportunities to develop familiarity and practical skills, but it can also increase exposure to harmful online interactions. For instance, among young internet users in Brazil, digital skills were associated with more online opportunities, and engagement with those opportunities was associated with greater exposure to risk (Cabello-Hutt et al., 2018). A systematic review similarly reported complex relationships among digital skills, opportunities, risks and well-being (Livingstone et al., 2023). While research in Asian low- and middle-income countries documents diverse forms of digitally mediated gender-based violence (Bansal et al., 2024), studies in sub-Saharan Africa identify the increased accessibility of potential victims and the rapid circulation of harmful content as key mechanisms facilitating this violence (Tarefa & Abdulai, 2026). More frequent use may therefore foster greater familiarity while simultaneously increasing risk exposure. This relationship, however, depends on the specific outcome examined. For example, across 37 European countries, Tang and Lu (2026) found that frequent internet use was associated with greater perceived safety in the local physical environment, although their study did not measure online safety specifically.

Previous experience of TFGBV is relevant to safety assessments. However, it differs from digital confidence and current perceptions of online safety. Measures of technology-facilitated violence capture different aspects of occurrence, frequency, severity, consequences and protective factors (Devereux et al., 2026). Definitions and measures also vary across low- and middle-income settings (Bansal et al., 2024). Previous victimisation may influence women's assessments of online environments, but does not establish their current confidence or safety perceptions. Similarly, the absence of reported victimisation does not demonstrate that a woman feels safe online. These dimensions require separate measurement and analysis.

Evidence on these relationships remains limited in sub-Saharan Africa. A scoping review identified 17 eligible studies, with the earliest published in 2019. Seven were conducted in Kenya, and university students featured prominently in the available research (Tarefa & Abdulai, 2026). Studies also focus on particular groups, including women journalists, women with disabilities and LGBTQI+ persons (Hameed et al., 2025; Ned et al., 2026). Their findings provide useful context, but leave questions about the relationships among capability, participation and perceived safety within a broader population of adult women.

Kenyan evidence demonstrates the relevance of these questions. A rapid study in institutions of higher learning found that nearly 90% of surveyed young adults in Nairobi had witnessed TFGBV and 39% had experienced this violence. Among female students, 64.4% reported at least one form of online violence (UNFPA, 2024). Subsequent national evidence reported lifetime TFGBV experience among 37.04% of respondents, while 13.16% of survivors had reported their experiences to authorities (UNFPA, 2025). Because the study populations differ, these figures should not be interpreted as directly comparable prevalence estimates. Civil society evidence also identifies online attacks, threats, harassment and intimidation affecting Kenyan women and girls, including women human rights defenders (Defenders Coalition, 2025). These findings support an examination of online safety that simultaneously considers individual capability and the conditions of digital participation.

In summary, the literature establishes the widespread occurrence and consequences of TFGBV (Bansal et al., 2024), its relevance in sub-Saharan Africa (Tarefa & Abdulai, 2026), and the importance of individual digital capability (Abima et al., 2021; Ulfert-Blank & Schmidt, 2022). It also identifies potential benefits of training (Khan et al., 2023), variations in risk associated with digital engagement (Livingstone et al., 2023), and limitations in wider protective systems (Pavón Pérez et al., 2026). However, a critical gap remains in understanding how these factors intersect to influence current safety perceptions among the general female population. The present study addressed this gap through four research questions examining training, confidence, internet use, previous TFGBV experience and perceived online safety.

Specifically, the study addressed the following research questions:

- i. Is formal digital safety training associated with digital confidence among adult women in Nairobi City County?
- ii. Is digital confidence associated with perceived online safety?
- iii. How are formal digital safety training and frequency of internet use associated with perceived online safety when considered simultaneously?
- iv. How are previous TFGBV experience and selected socio-demographic characteristics associated with perceived online safety?

RESEARCH METHODS

Study Design and Setting

The study used a cross-sectional survey design in Nairobi City County, Kenya. Nairobi comprises 17 sub-counties and has high levels of internet and mobile technology use, making it an appropriate setting for examining women's digital confidence and perceptions of online safety.

Study Population and Sampling

The study population comprised women aged 18 years and above who resided in Nairobi City County and had access to an internet-enabled mobile phone. A multistage sampling procedure was used across the county's 17 sub-counties. The sub-counties served as strata, with the sample allocated proportionately using population estimates from the Kenya National Bureau of Statistics. For field implementation, the sub-counties were organised into four geographical areas: North, East, North-West and South-West.

Within each sub-county, wards were selected through simple random sampling. Trained field researchers recruited participants at designated public locations using systematic sampling. Following a random start between 1 and 10, every tenth woman was approached and screened for eligibility. Eligible participants received a secure link to a self-administered online questionnaire, with one response permitted per participant.

Sample Size

The required sample size was estimated using Cochran's formula for large populations. Assuming a 95% confidence level, a 5% margin of error and a population proportion of .50, the estimated minimum sample was 385 participants. A total of 208 women completed the survey, representing 54.0% of the target sample.

Data Collection Instrument and Procedure

Data were collected between May and June 2026 using a structured, self-administered online questionnaire developed from the study objectives and relevant literature. The instrument covered

socio-demographic characteristics, digital media use, experiences of TFGBV, digital safety training, digital confidence and perceived online safety.

The questionnaire was reviewed by experts in gender-based violence and research methodology to assess content validity and was pretested before the main survey. Findings from the pretest informed revisions to the wording, formatting and ordering of questions. Internal consistency was assessed for the five-item measure of the perceived impact of TFGBV, which had high internal consistency in the study data (Cronbach's $\alpha = .926$). Eligible participants received information about the study and provided electronic informed consent before completing the questionnaire.

Measurement of Variables

Digital confidence captured participants' self-assessed capability to use digital technologies, navigate online environments and implement digital safety measures. Responses were recorded on a five-category ordered scale ranging from very low to very high. Higher categories represented greater digital confidence.

Perceived online safety, the principal outcome, assessed how safe participants felt when using digital platforms and internet-enabled technologies. Responses were recorded on five ordered categories ranging from *very unsafe* to *very safe*, with higher categories indicating greater perceived safety.

Formal digital safety training was assessed by asking participants whether they had received formal training in digital safety. Responses were coded as *yes* or *no*. Participants reporting training were also asked to identify the provider, including non-governmental organisations, online courses, employers, government agencies, schools or universities, and other providers. Provider information was used descriptively because the numbers within individual provider categories were insufficient for multivariable analysis.

Internet-use frequency was measured using five ordered categories: *less than once a week*, *once a week*, *several times a week*, *daily* and *constantly*. Higher categories represented more frequent internet use.

Previous TFGBV experience was defined as having experienced one or more forms of digitally mediated gender-based abuse assessed in the parent survey. Participants were classified as having experienced TFGBV or not, and the variable was included as an adjustment factor rather than as a primary outcome.

Selected socio-demographic characteristics were included as adjustment variables: age, highest educational attainment, employment status, perceived socio-economic status and marital status. Marital status was recoded as partnered (married or cohabiting) and not partnered (single,

divorced, separated or widowed). Non-substantive responses such as *prefer not to say* were treated as missing in multivariable analyses.

Data Analysis

Data were checked for completeness and consistency before analysis. Frequencies and percentages were used to describe digital confidence, formal digital safety training, internet-use frequency, perceived online safety, previous TFGBV experience and selected participant characteristics. Training providers were summarised descriptively among participants who reported receiving formal digital safety training.

The bivariate association between formal digital safety training and the five-category digital-confidence measure was examined using Pearson's chi-square test. Because digital confidence was ordinal, an ordinal logistic regression model was initially considered to assess its adjusted association with formal training while controlling for previous TFGBV experience, age, education, internet-use frequency, socio-economic status, marital status and employment status.

The proportional-odds assumption was assessed using a global parallel-slopes test before interpreting the ordinal model. The assumption was violated for digital confidence, $\chi^2(24) = 47.21$, $p = .003$. A single proportional-odds estimate was therefore not reported. Instead, adjusted cumulative binary logistic regression models were fitted at each of the four thresholds of the five-category confidence outcome: low to very high versus very low; moderate to very high versus low or very low; high or very high versus moderate or lower; and very high versus high or lower. Each model included the same adjustment variables, and results were expressed as odds ratios (ORs), 95% confidence intervals (CIs) and p -values.

The relationship between digital confidence and perceived online safety was first examined using Spearman's rank-order correlation because both variables were ordinal. An ordinal logistic regression model was then fitted with perceived online safety as the outcome. Digital confidence, formal digital safety training and internet-use frequency were the principal explanatory variables, with previous TFGBV experience, age, education, socio-economic status, marital status and employment status included as adjustment variables.

The proportional-odds assumption for the perceived-online-safety model was supported by the global parallel-slopes test, $\chi^2(27) = 26.46$, $p = .493$. The proportional-odds model was therefore retained. Adjusted ORs with 95% CIs and p -values were reported. For the ordered digital-confidence and internet-use variables, the OR represents the change in the odds of being in a higher outcome category associated with a one-category increase in the predictor, holding the other variables constant.

Multivariable analyses used complete cases. Participants selecting *prefer not to say* on variables required for a model were excluded from that analysis, resulting in 184 complete cases for the fully

adjusted models. Statistical significance was assessed at $p < .05$. Given the cross-sectional design, associations were interpreted as non-causal.

Ethical Considerations

Ethical approval and the necessary regulatory authorisations were obtained before data collection. Participation was voluntary, and all participants provided electronic informed consent before accessing the questionnaire. Participants could discontinue the survey at any stage. No residential addresses or unnecessary personally identifying information were collected, and study data were maintained confidentially with restricted access. Information on relevant support services was provided to participants because of the potentially sensitive nature of questions concerning online abuse.

RESEARCH RESULTS

Digital Confidence, Safety Training, Internet Use and Perceived Online Safety

A total of 208 women participated in the study. Digital confidence was generally high, with 58.2% reporting high or very high confidence and a further 34.6% reporting moderate confidence. Only 35.6% had received formal digital safety training. Internet use was frequent: 56.7% reported being constantly connected, and 33.7% used the internet daily. Perceptions of online safety were more reserved. Half of the participants (50.0%) felt neither safe nor unsafe, 23.1% felt safe or very safe, and 26.9% felt unsafe or very unsafe. Previous TFGBV experience was reported by 55.3% of participants. Table 1 presents the distributions of the main study variables.

Table 1 Digital Confidence, Formal Digital Safety Training, Internet Use, Perceived Online Safety and Previous TFGBV Experience (N = 208)

Variable	Category	<i>n</i>	%
Digital confidence	Very low	8	3.8
	Low	7	3.4
	Moderate	72	34.6
	High	69	33.2
	Very high	52	25.0
Formal digital safety training	No	134	64.4
	Yes	74	35.6
Internet-use frequency	Less than once a week	1	0.5
	Once a week	4	1.9
	Several times a week	15	7.2
	Daily	70	33.7
	Constantly	118	56.7
Perceived online safety	Very unsafe	11	5.3
	Unsafe	45	21.6
	Neither safe nor unsafe	104	50.0
	Safe	36	17.3
	Very safe	12	5.8
Previous TFGBV experience	No	93	44.7
	Yes	115	55.3

Note. Percentages may not total 100.0 because of rounding.

Among the 74 women who had received formal digital safety training, non-governmental organisations were the most frequently reported providers ($n = 20$), followed by online courses ($n = 18$), employers ($n = 13$), government agencies ($n = 11$) and schools or universities ($n = 9$). Two participants reported other providers, while provider information was missing for one participant.

Formal Digital Safety Training and Digital Confidence

The first research question examined whether formal digital safety training was associated with digital confidence. Digital confidence differed significantly by training status, $\chi^2(4) = 12.64$, $p = .013$. The proportional-odds assumption was then assessed before fitting the adjusted ordinal model. The global parallel-slopes test was significant, $\chi^2(24) = 47.21$, $p = .003$, indicating that the assumption was violated. Consequently, a single common odds ratio across the five digital-confidence categories was not retained. Instead, adjusted cumulative logistic models were examined separately across the four confidence thresholds.

As shown in Table 2, formal digital safety training was associated with higher odds of reporting high or very high digital confidence rather than moderate, low or very low confidence (OR = 2.69, 95% CI [1.32, 5.49], $p = .006$). Training was not significantly associated with the other three cumulative thresholds. Therefore, the association between formal training and digital confidence varied across the confidence distribution and did not conform to a single proportional-odds relationship.

Table 2

Adjusted Associations Between Formal Digital Safety Training and Cumulative Levels of Digital Confidence

Cumulative contrast	OR	95% CI	p
Low to very high vs very low	0.58	0.11–3.01	.514
Moderate to very high vs low/very low	2.01	0.51–7.83	.316
High/very high vs moderate/low/very low	2.69	1.32–5.49	.006
Very high vs high or lower	1.25	0.57–2.71	.578

Note. Complete-case N = 184. Models adjusted for TFGBV experience, age, education, internet-use frequency, socio-economic status, marital status and employment status. “Prefer not to say” responses were treated as missing. OR = odds ratio; CI = confidence interval.

Digital Confidence and Perceived Online Safety

The second research question examined whether digital confidence was associated with perceived online safety. Spearman’s rank-order correlation indicated a modest positive association between the two variables ($\rho = .211$, $p = .002$). Thus, higher digital confidence tended to correspond with greater perceived online safety.

As shown in Table 3, this association remained statistically significant after adjustment for formal digital safety training, internet-use frequency, previous TFGBV experience and the included socio-demographic characteristics. Each one-category increase in digital confidence was associated with 89% higher odds of being in a higher perceived-online-safety category (OR = 1.89, 95% CI [1.41, 2.54], $p < .001$).

Formal Digital Safety Training, Internet Use and Perceived Online Safety

The third research question examined the associations of formal digital safety training and internet-use frequency with perceived online safety when considered simultaneously with the other study variables.

Before interpreting the adjusted ordinal logistic regression, the proportional-odds assumption was assessed. The global parallel-slopes test was not statistically significant, $\chi^2(27) = 26.46$, $p = .493$, supporting the use of the proportional-odds model for perceived online safety.

Table 3 presents the fully adjusted results. Formal digital safety training was not independently associated with perceived online safety (OR = 1.56, 95% CI [0.87, 2.82], $p = .137$). Thus, although training was associated with the distribution of digital confidence, the adjusted analysis did not show an independent association between formal training and perceived online safety.

Internet-use frequency, in contrast, was independently associated with perceived online safety.

Each one-category increase in internet-use frequency was associated with 45% lower odds of being in a higher perceived-online-safety category (OR = 0.55, 95% CI [0.36, 0.83], $p = .005$), after adjustment for the other variables in the model.

Table 3 Adjusted Associations With Perceived Online Safety

Predictor	OR	95% CI	p
Digital confidence	1.89	1.41–2.54	< .001
Formal digital safety training	1.56	0.87–2.82	.137
Internet-use frequency	0.55	0.36–0.83	.005
Previous TFGBV experience	0.88	0.50–1.56	.671
Age	1.10	0.84–1.43	.487
Education	0.98	0.75–1.28	.899
Socio-economic status	1.23	0.62–2.44	.561
Partnered	0.94	0.52–1.69	.833
Employment status	0.80	0.37–1.76	.585

Note. Complete-case $N = 184$. Higher outcome categories indicate greater perceived online safety; digital confidence and internet-use frequency were ordered predictors. Partnered = married/cohabiting; “prefer not to say” = missing. OR = odds ratio; CI = confidence interval; TFGBV = technology-facilitated gender-based violence. The proportional-odds assumption was met, $\chi^2(27) = 26.46$, $p = .493$.

Previous TFGBV Experience, Socio-Demographic Characteristics and Perceived Online Safety

The fourth research question examined whether previous TFGBV experience and selected socio-demographic characteristics were associated with perceived online safety. After adjustment for digital confidence, formal digital safety training, internet-use frequency and the other variables in the model, previous TFGBV experience was not independently associated with perceived online safety (OR = 0.88, 95% CI [0.50, 1.56], $p = .671$).

None of the socio-demographic characteristics included in the model showed a statistically significant independent association with perceived online safety. These included age (OR = 1.10,

95% CI [0.84, 1.43], $p = .487$), education (OR = 0.98, 95% CI [0.75, 1.28], $p = .899$), socio-economic status (OR = 1.23, 95% CI [0.62, 2.44], $p = .561$), partnered status (OR = 0.94, 95% CI [0.52, 1.69], $p = .833$), and employment status (OR = 0.80, 95% CI [0.37, 1.76], $p = .585$).

Overall, digital confidence and internet-use frequency were independently associated with perceived online safety. In contrast, formal digital safety training, previous TFGBV experience and the measured socio-demographic characteristics were not.

RESEARCH DISCUSSION

The present study examined the relationships among formal digital safety training, digital confidence, internet-use frequency, and perceived online safety among adult women in Nairobi City County, Kenya. The findings revealed a key distinction between women's confidence in navigating digital environments and their perceptions of online safety. Although 58.2% of participants reported high or very high digital confidence, only 23.1% felt safe or very safe online. This disparity supports previous research that distinguishes digital self-efficacy from exposure to online risks (Ulfert-Blank & Schmidt, 2022; Livingstone et al., 2023). It shows that women may be confident in their digital skills while still concerned about their safety.

Digital confidence was positively associated with perceived online safety. Each one-category increase in confidence corresponded with 89% higher odds of reporting greater perceived safety (OR = 1.89, 95% CI [1.41, 2.54]). This finding is consistent with Bandura's (1997) self-efficacy theory, which emphasises the influence of perceived capability on individuals' responses to challenging situations. The finding also supports prior research distinguishing digital skills from perceived control over online risks (Helsper et al., 2025). Women with greater confidence may feel better equipped to recognise threats and adopt protective measures. However, the modest bivariate correlation suggests that confidence and perceived safety remain distinct constructs. The cross-sectional findings support an association between these constructs, rather than demonstrating that greater confidence produces greater safety.

Formal digital safety training was associated with high or very high confidence, but this association varied across the confidence distribution. Women who reported receiving training had 2.69 times the odds of reporting high or very high confidence rather than moderate or lower confidence. This finding corroborates prior research linking cybersecurity training to improved self-efficacy and protective knowledge (Khan et al., 2023; Anwar et al., 2017). It also aligns with research highlighting the importance of digital safety training among women journalists in Uganda (Kakooza & Kazibwe, 2025). However, the lack of significant associations at other confidence levels indicates that the relationship was not uniform. Self-selection into training offers another possible explanation, since women who are already confident or interested in digital safety may be more likely to seek training.

Despite its link to higher confidence, formal digital safety training showed no statistically significant independent association with perceived online safety. This finding suggests that enhancing individual capability does not necessarily lead to stronger perceptions of safety. Previous research identifies structural and institutional barriers that constrain women's ability to protect themselves from technology-facilitated violence (Henry et al., 2020, 2022). Structural vulnerabilities, combined with socio-economic disadvantages, increase exposure to harm and restrict access to digital justice, thereby limiting the capacity of individuals to protect themselves effectively (Hameed et al., 2025; Ned et al., 2026). Platform governance, regulatory frameworks and gendered power relations also influence online safety (Pavón Pérez et al., 2026; Sood, 2024). Therefore, while training may improve women's protective capabilities, it may not address the broader systemic factors contributing to online insecurity. These interpretations remain provisional, as the present study did not directly examine institutional responses, platform conditions, or the quality of training.

These findings have implications for evaluating digital safety interventions. Previous research shows that training can improve protective knowledge and self-efficacy (Khan et al., 2023). However, increased awareness may also help women recognise previously overlooked threats without necessarily improving their perceptions of safety. Training effectiveness should therefore be assessed through distinct measures of knowledge, practical skills, confidence and protective behaviour, alongside exposure to abuse and perceptions of institutional protection. Thus, the non-significant association between training and perceived safety should not be interpreted as evidence that training is ineffective.

Internet-use frequency was negatively associated with perceived online safety. Each one-category increase in frequency corresponded with 45% lower odds of reporting greater perceived safety (OR = 0.55, 95% CI [0.36, 0.83]). This finding supports previous research indicating that increased digital engagement creates opportunities while potentially increasing exposure to online risks (Cabello-Hutt et al., 2018; Livingstone et al., 2023). It is also consistent with evidence that different digital skills have different relationships with risk exposure (Ambahelagedara et al., 2026). Although much of this literature concerns younger populations and actual risk exposure, the present study extends the discussion to perceived online safety among adult women. Mechanisms identified in previous research, such as increased accessibility of potential victims and rapid circulation of harmful content, may account for this association (Bansal et al., 2024; Tarefa & Abdulai, 2026).

The negative association between internet-use frequency and perceived online safety observed in the current study contrasts with Tang and Lu's (2026) finding that frequent internet use was associated with greater perceived safety across European countries. However, their study examined perceptions of safety within local communities rather than online environments. The findings are therefore not directly contradictory but illustrate the importance of distinguishing

different dimensions of safety. Furthermore, the present study does not establish that frequent internet use causes insecurity. Digital technologies continue to provide women with opportunities for communication, information access and social support (Abima et al., 2021; Tyabashe-Phume et al., 2025). Therefore, digital safety interventions should strengthen protective conditions without discouraging women's digital participation.

Previous experience of TFGBV did not show a statistically significant independent association with perceived online safety. This finding does not contradict research documenting the consequences of victimisation. It should be interpreted alongside existing evidence documenting widespread online violence and limited reporting among women in Kenya (UNFPA, 2024, 2025). Previous studies have also identified psychological and educational consequences of online victimisation, particularly among younger populations (Ayodeji, 2025; Nkwanyana, 2026). The absence of a significant association may reflect differences between previous victimisation and current perceptions of safety. Additionally, the study's binary measure did not account for severity, frequency, nature or recency of abuse. In line with measurement concerns identified by Devereux et al. (2026), more nuanced assessments are necessary to establish how different victimisation experiences influence perceptions of online safety.

The study contributes to the regional literature, which has largely focused on university students and specific occupational groups (Tarefa & Abdulai, 2026). By simultaneously examining training, confidence, internet use and perceived safety, it extends Kenyan research on TFGBV exposure (UNFPA, 2024, 2025) and threats affecting women human rights defenders (Defenders Coalition, 2025). The findings also echo Ugandan research showing that digital participation can coexist with harassment and constraints on engagement among women journalists (Kakooza & Kazibwe, 2025; Walulya & Selnes, 2023). The main contribution is the demonstration of the distinct associations among measures that might otherwise be treated as equivalent indicators of digital safety.

For policy and practice, the findings support attention to individual capability alongside wider protective responses. While training is essential for strengthening individual capabilities, effective interventions should also address institutional and technological conditions that influence women's online experiences. As highlighted in research on institutional constraints and platform governance (Henry et al., 2022; Pavón Pérez et al., 2026), such interventions should incorporate accessible reporting mechanisms, responsive institutions, survivor support and stronger accountability from platforms. Training programmes should also be evaluated based on their content, duration, delivery methods and practical outcomes. To enhance women's digital participation, public institutions, technology providers, civil society and employers need to work together to ensure that the responsibility for preventing abuse does not fall only on individual users. Several limitations should be considered when interpreting these findings. The cross-sectional design prevents causal inference. Training, confidence and perceptions of safety may influence

one another. Confidence and perceived safety were measured using single self-report items, so confidence represents perceived capability rather than demonstrated performance. The training and victimisation indicators did not capture important differences in content or experience. Internet-use frequency did not distinguish platforms, activities or time spent online. Recruitment procedures requiring internet-enabled mobile phones and online questionnaire completion may also have excluded women with limited connectivity, digital literacy or mobility.

The achieved sample of 208 was below the target of 385, and adjusted analyses included 184 complete cases. These limitations may have reduced statistical precision and the ability to detect smaller associations. The exclusion of 24 respondents also introduces uncertainty regarding potential missing-data bias. Accordingly, the findings should be generalised beyond adult women in Nairobi with caution. Future research should employ longitudinal or intervention designs, validated multi-dimensional measures and incorporate practical assessments of digital capability. A more detailed examination of training characteristics, digital engagement, and victimisation experiences would provide stronger evidence to inform the development of interventions aimed at enhancing women's digital capabilities and online safety.

Conclusion

The present study examined the relationships among digital capability, engagement and perceived online safety among adult women in Nairobi City County, Kenya. Greater digital confidence was associated with higher perceived safety. Formal digital safety training was associated with high or very high confidence. Training did not show a statistically significant independent association with perceived safety. More frequent internet use was associated with lower perceived safety, while previous TFGBV experience and the measured socio-demographic characteristics did not show significant independent associations. The findings indicate that confidence and perceived online safety require separate attention in research and intervention design. Digital safety initiatives should develop women's protective capabilities alongside technological and institutional responses to online abuse. Longitudinal and intervention studies are needed to clarify the direction of these relationships and assess changes following training.

REFERENCES

- Abima, B., Engotoit, B., Kituyi, G. M., Kyeyune, R., & Koyola, M. (2021). Relevant local content, social influence, digital literacy, and attitude toward the use of digital technologies by women in Uganda. *Gender, Technology and Development*, 25(1), 87–111. <https://doi.org/10.1080/09718524.2020.1830337>
- Afifah, M., Ruhimat, R., & Setiawan, K. (2026). The effect of digital literacy on women's intentions to report gender-based violence among Womenspirasi Summit participants. *Priviet Social Sciences Journal*, 6(2), 375–391. <https://doi.org/10.55942/pssj.v6i2.1623>

- Ambahelagedara, H., Sortheix, F., Hietajärvi, L., & Ketonen, E. (2026). Navigating the digital maze: Understanding the interplay of digital skills and knowledge, online risks, and mental well-being among young people. *Computers in Human Behavior Reports*, 22, Article 101092. <https://doi.org/10.1016/j.chbr.2026.101092>
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. <https://doi.org/10.1016/j.chb.2016.12.040>
- Ayodeji, U. M. (2025). Examining the impact of technology-facilitated gender-based violence on the mental health and well-being of adolescents. *Current Journal of Applied Science and Technology*, 44(5), 66–77. <https://doi.org/10.9734/cjast/2025/v44i54537>
- Baekgaard, K. (2024). *Technology-facilitated gender-based violence: An emerging issue in women, peace and security*. Georgetown Institute for Women, Peace and Security. <https://giwps.georgetown.edu/resource/technology-facilitated-gender-based-violence/>
- Bandura, A. (1997). *Self-efficacy: The exercise of control*. W. H. Freeman.
- Bansal, V., Rezwan, M., Iyer, M., Leasure, E., Roth, C., Pal, P., & Hinson, L. (2024). A scoping review of technology-facilitated gender-based violence in low- and middle-income countries across Asia. *Trauma, Violence, & Abuse*, 25(1), 463–475. <https://doi.org/10.1177/15248380231154614>
- Cabello-Hutt, T., Cabello, P., & Claro, M. (2018). Online opportunities and risks for children and adolescents: The role of digital skills, age, gender and parental mediation in Brazil. *New Media & Society*, 20(7), 2411–2431. <https://doi.org/10.1177/1461444817724168>
- Defenders Coalition. (2025). *Position paper on technology facilitated gender-based violence (TFGBV)*. <https://defenderscoalition.org/report/position-paper-on-technology-facilitated-gender-based-violence-tfgbv/>
- Devereux, C., De Filippo, A., Namubiru, J., Salamanca, L., Isika, V. K., Chávez-Lazo, A., & Hatcher, A. M. (2026). *Understanding and measuring technology-facilitated gender-based violence (TF-GBV): A guide to quantitative assessment tools*. Innovations for Poverty Action & sistemaFutura.
- Dunn, S. (2020). *Technology-facilitated gender-based violence: An overview* (Supporting a Safer Internet Paper No. 1). Centre for International Governance Innovation. <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/>
- Hameed, S., Tyabashe-Phume, B., Tunggal, E., Hunt, X., Ned, L., & Soldatić, K. (2025). Technology-facilitated gender-based violence against women with disabilities in low- and middle-income countries: A scoping review protocol. *BMJ Open*, 15(3), Article e093988. doi.org/10.1136/bmjopen-2024-029398
- Helsper, E. J., Veltri, G. A., & Livingstone, S. (2025). Parental mediation of children's online risks: The role of parental risk perception, digital skills and risk experiences. *New Media & Society*, 27(11), 5986–6005. <https://doi.org/10.1177/14614448241261945>
- Henry, N., Flynn, A., & Powell, A. (2020). Technology-facilitated domestic and sexual violence: A review. *Violence Against Women*, 26(15–16), 1828–1854. <https://doi.org/10.1177/1077801219875821>

- Henry, N., Vasil, S., Flynn, A., Kellard, K., & Mortreux, C. (2022). Technology-facilitated domestic violence against immigrant and refugee women: A qualitative study. *Journal of Interpersonal Violence*, 37(13–14), NP12634–NP12660. <https://doi.org/10.1177/08862605211001465>
- Jankowicz, N., Gomez-O’Keefe, I., Hoffman, L., & Vidal Becker, A. (2024). *It’s everyone’s problem: Mainstreaming responses to technology-facilitated gender-based violence*. Institute of Global Politics, Columbia University School of International and Public Affairs. https://igp.sipa.columbia.edu/sites/igp/files/2024-09/IGP_TFGBV_Its_Everyones_Problem_090524.pdf
- Kakooza, F., & Kazibwe, S. (2025). Digital safety: Perspectives from women journalists in Uganda. In M. Jjuuko, S. Omland, & C. A. Dralega (Eds.), *Gender and media representation: Perspectives from Sub-Saharan Africa* (pp. 161–174). Emerald Publishing. <https://doi.org/10.1108/978-1-83608-406-820251012>
- Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick’s model. *Computers & Security*, 125, Article 103049. <https://doi.org/10.1016/j.cose.2022.103049>
- Koch, L., Russo Riva, M. P., & Steinert, J. I. (2026). Technology-facilitated gender-based violence against politically active women: A systematic review of psychological and political consequences and women’s coping behaviors. *Trauma, Violence, & Abuse*, 27(4). <https://doi.org/10.1177/15248380251343185>
- Liu, S., Li, Y., Wen, H., & Wang, Y. (2026). Can digital literacy alleviate the multi-dimensional inequalities among rural residents? Evidence from China. *Sustainability*, 18(2), Article 1069. <https://doi.org/10.3390/su18021069>
- Livingstone, S., Mascheroni, G., & Stoilova, M. (2023). The outcomes of gaining digital skills for young people’s lives and well-being: A systematic evidence review. *New Media & Society*, 25(5), 1176–1202. <https://doi.org/10.1177/14614448211043189>
- Ned, L., Tyabashe-Phume, B., Tungal, E., & Soldatić, K. (2026). A baseline quantitative analysis of technology-facilitated gender-based violence against women with disabilities in South Africa. *Behavioral Sciences*, 16(5), 745. <https://doi.org/10.3390/bs16050745>
- Nkwanyana, B. P. (2026). Technology-facilitated gender-based violence and cyberbullying in secondary schools. *International Journal of Studies in Psychology*, 1(1si), 56–64. <https://doi.org/10.66434/ijpsy.v1i1si.498>
- Pavón Pérez, Á., Farrell, T., De Kock, C., Jurasz, O., Nozza, D., & Fernandez, M. (2026). Still unsafe: What’s holding us back on online safety for women. *AI and Ethics*, 6, Article 246. <https://doi.org/10.1007/s43681-026-01097-0>
- Sood, A. (2024). Technology-facilitated gender-based violence in India. In R. Sinha & P. Basu (Eds.), *Family and gendered violence and conflict* (pp. 455–475). Springer. https://doi.org/10.1007/978-3-031-60383-9_25
- Tang, X., & Lu, G. (2026). Perceived safety in digital information environments: Objective violence, online disinformation, internet use, and victimisation across Europe, 2002–2023. *Frontiers in Psychology*, 17, Article 1918767. <https://doi.org/10.3389/fpsyg.2026.1918767>

- Tarefa, Y. A., & Abdulai, A.-F. (2026). Technology-facilitated gender-based violence against women and girls in sub-Saharan Africa: A scoping review. *PLOS ONE*, 21(8), e0354526. <https://doi.org/10.1371/journal.pone.0354526>
- Tyabashe-Phume, B. P., Tunggal, E., Hameed, S., Hunt, X., Soldatić, K., & Ned, L. (2025). Scoping review on technology-facilitated gender-based violence against women with disabilities and LGBTQI+ persons in low- and middle-income countries. *African Journal of Disability*, 14, Article a1810. <https://doi.org/10.4102/ajod.v14i0.1810>
- Ulfert-Blank, A.-S., & Schmidt, I. (2022). Assessing digital self-efficacy: Review and scale development. *Computers & Education*, 191, Article 104626. <https://doi.org/10.1016/j.compedu.2022.104626>
- UN Women. (2025, November 13). *FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women and girls*. <https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women>
- United Nations Population Fund. (2024). *Rapid study on technology-facilitated gender-based violence (TFGBV) in Kenya's higher learning institutions*. UNFPA Kenya.
- United Nations Population Fund. (2025). *Making All Spaces Safe (MASS) programme in Kenya*. UNFPA Kenya. <https://kenya.unfpa.org/en/making-all-spaces-safe-in-kenya>
- Walulya, G., & Selnes, F. N. (2023). "I thought you are beautiful": Uganda women journalists' tales of mob violence on social media. *Digital Journalism*, 11(10), 1962–1981. <https://doi.org/10.1080/21670811.2023.2170899>