



JURNAL KOMUNIKASI

P-ISSN: 1907-848X, E-ISSN: 2548-7647

Homepage: <https://journal.uui.ac.id/jurnal-komunikasi>

Digital skill and digital safety in combating online fraud: A cross-generational study

**Febri Nurrahmi, Cut Lusi Chairun Nisak, Tanzir Masykar &
Ashabul Yamin Asgha**

To cite this article:

Nurrahmi, F. ., Nisak , . C. L. C. ., Masykar, T., & Asgha , A. Y. . (2025). Digital skill and digital safety in combating online fraud: A cross-generational study. Jurnal Komunikasi, 19(3), 559–572. <https://doi.org/10.20885/komunikasi.vol19.iss3.art8>



© 2025 The Author(s). Published by the Department of Communications,
Universitas Islam Indonesia, Yogyakarta, Indonesia.



Published online: October 31, 2025



[Submit your article to this journal](#)



To link to this article: <https://doi.org/10.20885/komunikasi.vol19.iss3.art8>



CrossMark

[View Crossmark data](#)



Digital skill and digital safety in combating online fraud: A cross-generational study

Febri Nurrahmi^{1*}, Cut Lusi Chairun Nisak², Tanzir Masykar³ &
Ashabul Yamin Asgha⁴

¹ Department of Communication, FISIP, Universitas Syiah Kuala, Banda Aceh, Indonesia.
Email: febri.nurrahmi@usk.ac.id

² Department of Sociology, FISIP, Universitas Syiah Kuala, Banda Aceh, Indonesia.
Email: cutlusi@usk.ac.id

³ Department of Metal Welding Technology, Akademi Komunitas Negeri Aceh Barat, Aceh Barat, Indonesia. Email: tanzir@akanacehbarat.ac.id

⁴ Department of Communication, FISIP, Universitas Teuku Umar, Aceh Barat, Indonesia.
Email: ashabulyaminasgha@utu.ac.id

* Corresponding author

Article Info

Article History

Submitted:

July 31, 2025

Accepted:

October 16, 2025

Published:

October 31, 2025

Keywords:

Digital safety,
digital skill,
generational
differences,
online fraud

Kata kunci:

Keamanan
digital,
keterampilan
digital,
perbedaan
generasi,
penipuan online

Abstract: Aceh reported 1,987 cases of illegal financial activities between November 2024 and May 2025. This study examines the levels of digital skill and digital safety among Gen X, Gen Y, and Gen Z in the context of online fraud. A total of 300 Acehnese respondents aged 17–60 years participated in the study. Data were collected through an online survey using a questionnaire distributed via Google Forms. The data were further analyzed using descriptive statistics and the Kruskal–Wallis test in SPSS version 22. The results showed generational differences in digital skills and digital safety. Gen Y achieved the highest scores in both domains, followed by Gen Z with slightly lower results. At the same time, Gen X consistently reported the lowest. Across all groups, digital safety scores lagged behind digital skill scores. Strengthening digital safety awareness is therefore crucial to reducing vulnerability to online fraud.

Abstrak: Aceh melaporkan 1.987 kasus aktivitas keuangan ilegal antara November 2024 hingga Mei 2025. Penelitian ini mengkaji tingkat digital skill dan digital safety di antara Gen X, Gen Y, dan Gen Z dalam konteks penipuan online. Sebanyak 300 responden asal Aceh berusia 17–60 tahun berpartisipasi dalam penelitian ini. Data dikumpulkan melalui survei online menggunakan kuesioner yang disebar via Google Forms. Data kemudian dianalisis dengan statistik deskriptif dan uji Kruskal–Wallis menggunakan SPSS versi 22. Hasil penelitian menunjukkan adanya perbedaan antar generasi dalam digital skill dan digital safety. Gen Y memperoleh skor tertinggi pada kedua domain, diikuti oleh Gen Z dengan skor lebih rendah, sementara Gen X secara konsisten memperoleh skor terendah. Pada semua kelompok, digital safety lebih rendah dibandingkan skor digital skill. Oleh karena itu, penguatan kesadaran digital safety menjadi sangat penting untuk mengurangi kerentanan terhadap penipuan online.

INTRODUCTION

Various forms of fraud, including phishing, investment scams, e-commerce fraud, and identity theft, continue to evolve alongside the growing reliance on digital technology. In Indonesia, reports of online fraud are increasing, with a wide range of schemes targeting internet users across age groups. A national study on digital fraud in Indonesia by Universitas Gadjah Mada (UGM) revealed the public's vulnerability, with 66.6% of respondents having been victims (Kurnia et al., 2022). The most common fraud schemes include scams via SMS/phone calls, prize hoaxes, and scams through suspicious links.

In facing this challenge, digital literacy plays a crucial role in building public resilience against online fraud (Li et al., 2024). Digital literacy is not limited to technical skills in using digital tools, but also includes critical understanding of information and the ability to evaluate source credibility (Syam & Nurrahmi, 2020). In the context of data protection, digital literacy is essential in preventing personal data breaches (Saputra, 2023). Adequate digital safety knowledge, such as the ability to secure social media accounts and avoid oversharing, can help individuals stay protected from digital threats (Mesch & Dodel, 2018). Without sufficient digital literacy, internet users are more likely to fall victim to online scams, either due to a lack of awareness or a limited understanding of how to protect themselves (Shao et al., 2019). In this context, Protection Motivation Theory (PMT) provides a valuable framework for examining the gap between digital skills and digital safety. While digital skills reflect users' technical ability to operate online tools, digital safety involves protective behaviors such as verifying messages, applying security measures, and avoiding risky practices. PMT explains that

protective behavior depends not only on coping resources (such as technical skills) but also on threat appraisal (perceived severity and vulnerability) and coping appraisal (self-efficacy and response efficacy) (Tsai et al., 2016). This perspective helps clarify why individuals who are proficient in using digital technologies may still hesitate to adopt preventive measures.

Despite the recognized importance of digital literacy in combating online fraud, no study has explicitly measured digital safety and digital skills across different generations in Indonesia. Existing research still tends to focus on legal or descriptive aspects of online fraud (Farhani & Isnawati, 2023; Kamran & Maskun, 2021; Puspitasari, 2018; Rahmad, 2019). A national-scale study on online fraud in Indonesia, involving 1,700 respondents across 34 provinces, yielded only descriptive results on incidents, channels, victims, losses, and recommendations (Kurnia et al., 2022). Meanwhile, digital literacy campaigns such as the *Gerakan Nasional Literasi Digital* (GNLD) have reportedly reached over 24 million people (Hikmah et al., 2024). However, the persistent rise in fraud cases suggests that these efforts are not sufficiently tailored to online fraud.

Aceh was selected as the research site due to the alarming rise of online fraud cases in the region. Data from the Indonesian Financial Services Authority (*Otoritas Jasa Keuangan*, OJK) show that between November 2024 and May 2025, there were 1,987 reports of illegal financial fraud in Aceh (Antara News Aceh, 2025). In June 2025 alone, OJK Aceh recorded 84 cases of illegal financial activities, including 32 investment scams and 52 illegal online lending cases (The Aceh Post, 2025). These figures highlight the region's vulnerability to digital fraud, underscoring

a pressing need for improved digital literacy in the region.

Previous research shows that attitudes and behaviors toward cybersecurity differ across generations. Older cohorts, such as Baby Boomers and Gen X, tend to fear cybercrime more due to perceived vulnerability and limited technological experience, yet they are less confident and perform fewer protective behaviors (Jiang et al., 2016; Wongmahesak et al., 2025). Conversely, younger generations, often labeled digital natives, are more comfortable with technology but often underestimate their risks, leading to riskier online behaviors (Robinson et al., 2020). Studies also indicate that Gen Y demonstrates stronger cybersecurity practices than Gen Z, likely due to greater experience and reduced perceptions of invulnerability (Debb et al., 2020). Therefore, this study aims to examine the levels of digital safety and digital skills among Gen X, Gen Y, and Gen Z in dealing with online fraud. Understanding generational gaps in protective online behaviors is essential for designing effective, age-specific educational interventions that can strengthen digital resilience and reduce vulnerability to fraud.

Based on previous literature and to answer the research objectives, the following hypotheses are proposed:

- H1: There are significant differences in digital skill levels across Gen X, Gen Y, and Gen Z.
- H2: There are significant differences in digital safety levels across Gen X, Gen Y, and Gen Z.

METHOD

This study employed a quantitative approach to examine the levels of digital skills and digital safety across three generations: Gen X, Gen Y, and Gen Z. Data were collected through an online survey administered via Google Forms and distributed through WhatsApp from August 18 to 30, 2025.

The population consisted of Acehnese individuals residing in Aceh Province whose national identity cards listed Banda Aceh, Aceh Besar, Lhokseumawe, Aceh Utara, Aceh Tengah, or Aceh Barat as their place of residence. Participants were aged 17–60 years, categorized as Gen Z (17–28 years), Gen Y (29–44 years), and Gen X (45–60 years). As a complete sampling frame was unavailable, a non-probability sampling method, namely convenience sampling, was employed. Respondents were selected non-randomly based on accessibility and willingness to participate (Golzar et al., 2022). Participation was voluntary and anonymous.

The questionnaire began with informed consent and consisted of three sections. The first gathered demographic data, while the following two measured digital skills and digital safety using a 4-point Likert scale (1 = strongly disagree to 4 = strongly agree), eliminating neutral responses. Items were adapted from the Digital Literacy Index (Kominfo & Katadata Insight Center) and modified to reflect the online fraud context, with additional adjustments from van 't Hoff-de Goede et al. (2025). The instrument was validated by two experts in digital literacy and psychometric assessment to ensure content validity.

To ensure content validity, the questionnaire was reviewed by two experts, one in digital literacy and another in psychometric measurement, who assessed item clarity, relevance, and appropriateness. Quantitative data were analyzed using SPSS version 22. Reliability testing with Cronbach's Alpha indicated strong internal consistency for the 11-item Digital Skill scale ($\alpha = 0.925$) and acceptable reliability for the revised 8-item Digital Safety scale ($\alpha = 0.772$). Construct validity was supported by the Kaiser-Meyer-Olkin (KMO) and Bartlett's tests, confirming adequate sampling and factorability. Overall, both instruments were deemed reliable and valid for measuring digital skills and digital safety in the context of online fraud protection.

Descriptive statistics were used to describe respondents' digital literacy levels. Differences across generational groups were analyzed using the non-parametric Kruskal–Wallis test due to non-

normal data distribution (Ostertagová et al., 2014), followed by Dunn's post-hoc test to identify specific group differences.

RESULTS AND DISCUSSION

Profile of the Respondents

This study involved 300 respondents representing a diverse demographic profile. The majority were female and predominantly from the millennial age group (Gen Y, aged 29–44 years). Most respondents resided in Banda Aceh and Aceh Besar, reflecting the higher population concentration and accessibility of these areas. In terms of occupation, civil servants and students made up the most significant proportion, indicating that the sample was primarily composed of individuals actively engaged in the public sector or higher education. Regarding educational background, most participants held at least a bachelor's degree (S1), indicating a relatively high level of formal education among the respondents.

Table 1

The respondents' profile

Characteristics	N (%)
Gender	
Female	195 (65%)
Male	105 (35%)
Age groups	
Gen X	63 (21%)
Gen Y	131 (43.7%)
Gen Z	106 (35.3%)
District	
Banda Aceh	153 (51%)
Aceh Besar	64 (21.3%)
Aceh Barat	35 (11.7%)
Aceh Tengah	22 (7.3%)
Lhokseumawe	16 (5.3%)
Aceh Utara	10 (3.3%)
Education	
Junior high school	11 (0.36%)
Senior high school	91 (30.4%)
Diploma	10 (0.33%)
Bachelor's degree	100 (33.3%)
Master's degree	79 (26.3%)
Doctoral degree	9 (0.3%)
Occupation	
Government employee	89 (29.7%)
Private employee	39 (13%)
Self-employed	15 (5%)
Homemaker	35 (11.6%)
Student	80 (26.7%)
Retired	1 (0.3%)
Unemployed	4 (1.3%)
Other	37 (12.3%)

Source: data analysis results

Descriptive Analysis of Digital Skills and Digital Safety

The descriptive analysis of respondents' digital skills, measured on a 4-point Likert scale, demonstrates a generally high level of perceived competence across various aspects of digital skills. The analysis of the individual items revealed distinct patterns of competence among respondents. The highest mean score was found in the ability to interact using digital technology devices

such as computers, smartphones, and tablets ($M = 3.55$, $SD = 0.65$), followed by creating a PIN or password to unlock a phone screen ($M = 3.51$, $SD = 0.79$) and using fingerprint authentication features ($M = 3.45$, $SD = 0.82$). These results suggest that participants were highly proficient in fundamental digital interactions and everyday device security measures, which are frequently practiced in daily life.

Similarly, skills such as searching and accessing digital content ($M = 3.42$, $SD = 0.72$), using the face authentication feature ($M = 3.32$, $SD = 0.88$), and verifying the trustworthiness of online information ($M = 3.24$, $SD = 0.80$) also scored relatively high. Respondents also reported being able to back up data to storage media ($M = 3.21$, $SD = 0.88$), upload files to the internet safely ($M = 3.19$, $SD = 0.76$), and download files securely ($M = 3.13$, $SD = 0.79$). On the lower end, enabling two-factor authentication ($M = 3.08$, $SD = 0.95$) and installing and using

antivirus software ($M = 2.96$, $SD = 0.88$) received the lowest mean scores. These findings reveal a gap between basic operational skills and the higher-level protective competencies essential for preventing cyber risks.

Overall, the digital skill scores ranged from 11 to 44, with an average of 36.06 ($SD = 6.77$), showing a high level of competence among respondents. However, there remains a gap in advanced security practices that are crucial for ensuring comprehensive digital safety.

Table 2
Digital skill

Items	Mean	Std. Deviation
I can verify whether the information I find on websites is trustworthy or not	3.24	0.80
I can search for and access data, information, and digital content as needed	3.42	0.72
I can upload files to the internet safely	3.19	0.76
I can download files from the internet safely	3.13	0.79
I can interact using digital technology devices (computer, smartphone, tablet)	3.55	0.65
I can install and use antivirus software	2.96	0.88
I can create a PIN or password to unlock my phone screen	3.51	0.79
I can use the fingerprint authentication feature	3.45	0.82
I can use the face authentication feature	3.32	0.88
I can back up data to a backup storage	3.21	0.88
I can enable two-factor authentication	3.08	0.95
Overall digital skill	36.06	6.77

Source: data analysis results

The descriptive analysis of respondents' digital safety practices, measured on a 4-point Likert scale, indicates a moderate level of awareness and behavior, with some variation across specific areas. Looking at the individual items, the highest mean score was found in "I immediately delete messages that I consider suspicious" ($M = 3.31$, $SD = 0.90$), suggesting that most respondents are proactive in removing potentially harmful content. This was followed by "I am selective when accepting friend requests on social media" ($M = 3.08$, $SD = 1.01$),

showing a cautious approach to online social interactions.

Respondents also demonstrated relatively strong practices in "I back up my important files" ($M = 2.92$, $SD = 0.94$) and "On my social media account, I can control who sees my posts (timeline)" ($M = 2.89$, $SD = 1.06$), reflecting awareness of both data protection and privacy settings. Similarly, "I can disable the option to show my geographical location/GPS" ($M = 2.77$, $SD = 0.96$) and "I back up or save data in multiple locations" ($M = 2.74$, $SD = 0.93$) received moderate scores, indicating that

while these practices are known, they may not yet be consistently applied.

Lower mean scores were observed in “If I doubt the authenticity of a message, I contact the sender to verify whether they really sent the email” ($M = 2.51$, $SD = 1.04$) and “I use applications to detect and remove viruses on all my devices” ($M = 2.37$, $SD = 0.96$). These results suggest weaker habits in verification and device protection, highlighting areas that require improvement.

Overall, respondents scored 22.58 ($SD = 4.85$) on a scale of 8–32, reflecting a moderate level of digital safety practices. Respondents demonstrate a reasonably good level of digital safety, particularly in deleting suspicious messages and being selective in social media interactions. However, gaps remain in more preventive and technical practices, such as verifying suspicious messages with senders, using antivirus applications, and consistently backing up data in multiple locations.

Table 3
Digital safety

Items	Mean	Std. Deviation
I back up my important files	2.92	0.94
I back up or save data in multiple locations	2.74	0.93
I use applications to detect and remove viruses on all my devices	2.37	0.96
I am selective when accepting friend requests on social media	3.08	1.01
On my social media account, I can control who sees my posts (timeline)	2.89	1.06
I can turn off the option to show my geographical location/GPS	2.77	0.96
I immediately delete messages that I consider suspicious	3.31	0.90
If I doubt the authenticity of a message, I contact the sender to verify whether they really sent the email	2.51	1.04
Overall digital safety	22.58	4.85

Source: data analysis results

Generational Differences in Digital Skill and Digital Safety

The results in Table 4 show apparent generational differences in digital skills. Gen Y achieved the highest mean score ($M = 37.60$, $SD = 5.89$), followed closely by Gen Z ($M = 36.87$, $SD = 6.31$). These findings indicate that both groups perceive themselves as having relatively

strong digital abilities. In contrast, Gen X reported a considerably lower mean score ($M = 31.48$, $SD = 7.29$), suggesting more limited confidence in their digital skills. This pattern highlights a possible age-related gap, where younger generations demonstrate stronger digital competence compared to older cohorts.

Table 4
Digital skills according to age groups

Age Groups	N	Mean	Std. Deviation
Gen Z	106	36.87	6.31
Gen Y	131	37.60	5.89
Gen X	63	31.48	7.29

Source: data analysis results

The Kruskal–Wallis test revealed significant differences in digital skill across generations ($\chi^2 = 36.22$, $p < 0.001$). Post hoc analysis using Dunn's test showed that the differences were significant between Gen Z and Gen X, as well as between Gen Y and Gen X. The results indicated that both younger generations reported higher levels of digital skill compared to Gen X. However, no significant difference was found between Gen Z and Gen Y, suggesting that these two younger groups share relatively similar levels of digital competence.

The Kruskal–Wallis test on individual digital skill items indicated significant generational differences across all items. Post hoc analysis revealed significant differences between Gen Z and Gen X, as well as between Gen Y and Gen X, for Items 1, 2, 5, 6, 7, 8, 9, 10, and 11, with

younger generations reporting higher skill levels. For Item 3, "I can upload files to the internet safely," the difference was significant only between Gen Y and Gen X.

Subsequently, Table 5 presents the mean digital safety scores across age groups, measured on a scale from 8 to 32. Descriptive results show that Gen Y reported the highest mean score ($M = 24.05$, $SD = 4.13$), indicating stronger engagement in digital safety practices. Gen Z followed closely ($M = 22.70$, $SD = 4.18$), reflecting a moderate level of digital safety. In contrast, Gen X had the lowest mean score ($M = 19.37$, $SD = 5.74$), suggesting weaker digital safety practices compared to the younger generations. This trend points to a generational gap, with older adults being less active in applying digital safety measures, while Gen Y stands out slightly ahead.

Table 5
Digital safety according to age groups

Age Groups	N	Mean	Std. Deviation
Gen Z	106	22.70	4.18
Gen Y	131	24.05	4.13
Gen X	63	19.37	5.74

Source: data analysis results

A Kruskal–Wallis test revealed a statistically significant difference in digital safety scores among the three age groups ($\chi^2 = 29.03$, $p < 0.001$). Post-hoc comparisons using Dunn's method found significant differences between Gen Z and Gen X, as well as between Gen Y and Gen X. This implies that younger generations (Gen Z and Gen Y) tend to demonstrate stronger digital safety practices compared to Gen X, who reported the lowest scores.

Further item-level analysis highlighted that digital safety behaviors differed significantly across age groups. The post hoc Dunn's test provided more

detailed insights into which generational groups differed significantly across individual digital safety items. For Safety 3 (backing up important files), Safety 4 (backing up or saving data in multiple locations), and Safety 8 (controlling social media visibility), significant differences were found between Gen Z and Gen X, as well as between Gen Y and Gen X. Similarly, for Safety 5 (using antivirus applications) and Safety 10 (deleting suspicious messages), significant differences emerged between Gen Y and Gen X. Interestingly, Safety 7 (being selective with friend requests) showed

significant differences across all three generational groups, indicating varying levels of cautiousness in managing social connections online. For Safety 11 (contacting senders to verify suspicious messages), a significant difference was observed between Gen Z and Gen Y. In contrast, Safety 9 (disabling GPS location settings) showed no significant differences across generations, suggesting relatively similar practices in this domain.

These results highlight that Gen X consistently scored lower in preventive and protective behaviors, while Gen Z and Gen Y demonstrated stronger practices. However, certain safety behaviors, such as managing GPS settings, appear to be adopted similarly across generations.

Comparative Analysis of Digital Skills and Digital Safety Among Generations

The Kruskal–Wallis test confirmed that digital skills vary significantly across generations. Follow-up analysis with Dunn's test indicated notable differences between Gen Z and Gen X, as well as between Gen Y and Gen X. Younger cohorts consistently demonstrated higher digital skill levels than Gen X. This is consistent with Long et al. (2023), who found that older individuals (aged 55+) have significantly lower digital literacy than younger individuals (aged 15–24). However, no significant difference was found between Gen Z and Gen Y, suggesting that these two younger groups share relatively similar levels of digital competence. The comparable digital skill score of Gen Y and Gen Z can be explained by the fact that Gen Y were early adopters of online technologies, while Gen Z grew up fully digital (Putra, 2017). Both generations are thus accustomed to navigating online spaces.

The study also found that Gen X had lower digital skill scores compared to Gen Y and Gen Z. This finding can be explained by the fact that Gen X is classified as digital immigrants, as they were first exposed to digital technologies in adulthood (Çoklar & Tatli, 2021). Consequently, their overall digital competence tends to be lower than that of younger generations who have grown up in a digital environment. It is also important to note that the inclusion of Baby Boomers might have revealed a wider gap in digital skills. Jiang et al. (2016) found that this generation generally lacks digital competence.

A closer look at the mean scores for individual digital skill items shows an interesting trend. Basic security features, such as creating a PIN or password ($M = 3.51$), using fingerprint authentication ($M = 3.45$), and face authentication ($M = 3.32$), received relatively high scores. However, as the technologies become more advanced, the average scores tend to decline. For example, enabling two-factor authentication scored the lowest ($M = 3.08$). This suggests that while most users are familiar with basic digital security practices, their use of more advanced tools is still limited. Ironically, two-factor authentication is one of the most effective ways to prevent data breaches (Adeoye, 2012).

Uploading and downloading files from the internet safely were among the lower-rated skills, ranking as the second- and third-lowest mean scores. Although still within a relatively high range, these findings may suggest limited experience in managing file transfers online. This may also reflect users' limited ability to identify secure websites or verify the safety of links. Cybercriminals often exploit file transfers to spread malware or launch phishing attacks disguised as legitimate documents

(Alawida et al., 2022). Using untrusted or unsecured platforms for file exchange increases the risk of data theft (Puram et al., 2011). A lack of digital skills in these specific areas can make users more vulnerable to such online fraud.

The lowest mean score was observed for the skill “I can install and use antivirus software.” Cost has been identified as a deterrent factor for using antivirus software (Rowe et al., 2012). In fact, previous research showed that the proper implementation of antivirus programs can reduce the negative impact of malicious attacks on computer systems (Jovanović et al., 2024).

In terms of overall digital safety scores, Gen Y scored the highest and were categorized as having high digital safety, while both Gen Z and Gen X showed moderate levels. Gen Y appeared to be more proactive in addressing potential threats than the older generations (Jiang et al., 2016). Although no studies have specifically compared digital safety across generations, Gen Y's higher scores may be explained by their lower likelihood of falling victim to online scams. This is consistent with findings from a monograph on online scams, which reported that Gen Y were the least likely to become victims of digital fraud (Kurnia et al., 2022). Interestingly, Gen Z reported high digital skills but only moderate digital safety. This gap suggests that technical ability does not automatically translate into safer online behavior. Their moderate safety score may be linked to a firm trust in technology (Agrawal et al., 2025). Moreover, Gen Z's constant use of technology across various devices and daily activities increases their exposure to potential threats. Ribeiro et al. (2024) found that individuals who engage heavily in routine online activities are more susceptible to phishing attacks. This aligns with data showing that Gen Z in Indonesia is the second most frequent target of digital

scams, following Baby Boomers (Kurnia et al., 2022).

The low score on verifying suspicious messages ($M = 2.51$) indicates that many users overlook message authenticity, leaving them vulnerable to phishing. Moreover, the lowest score ($M = 2.37$) on using antivirus tools reflects weak habits in device protection. This is consistent with the lowest score of digital skills for installing antivirus software. This suggests that using antivirus software requires more technical knowledge and is less frequently practiced in daily life.

In general, this study found that the average digital safety score was lower than the digital skill score. This finding is consistent with previous research (Dinas Komunikasi dan Informatika Kabupaten Sleman, 2022; Nisa et al., 2023; Sanjaya et al., 2024). This gap may contribute to the high incidence of online fraud in Aceh. One possible explanation for this gap is that while individuals may be proficient in using digital tools and platforms, they may not be as concerned about online threats.

From the perspective of Protection Motivation Theory (PMT), digital skills can be seen as a coping resource, whereas digital safety reflects protective behavior. Although individuals are proficient in using digital tools, they may underestimate the severity and likelihood of online threats (low threat appraisal) or doubt their ability to apply protective measures such as verifying suspicious messages and using antivirus software (low coping appraisal). As a result, digital safety is not prioritized in daily practice despite high levels of digital skill.

While offering valuable insights, this study has several limitations. First, the data were not normally distributed, which may have affected the robustness of the statistical analysis. This may reduce the strength of group comparisons. Second, the study relied on self-reported data. Such

data may be biased and may not accurately reflect actual behaviors.

CONCLUSION

Unlike most studies focusing on legal or descriptive aspects of online fraud, this study quantitatively demonstrates generational differences in digital skills and safety. This study shows that Gen Y achieved the highest scores in both digital skills and digital safety. Gen Z followed with slightly lower results. At the same time, Gen X consistently reported the lowest scores. The gap is consistent across most items, although some practices are adopted in a similar manner. No significant difference was found between Gen Z and Gen Y, indicating that the two younger groups share comparable competence. It also reveals that digital safety awareness lags behind digital skills in all groups.

The findings have theoretical value. They confirm that digital competence and digital safety are not the same. Strong skills in using digital tools do not guarantee strong safety practices. This supports PMT by showing that coping resources (digital skills) are not sufficient to translate into protective actions. Models of digital literacy should therefore separate operational competence from protective behaviors. In addition, this study contributes by developing an instrument to measure digital skills and digital safety in the context of online fraud. This tool can support future research and provide a basis for designing more precise interventions.

Practical implications are evident. Digital literacy programs can use these generational differences to design more targeted interventions against online fraud. Training should go beyond basic device use and focus on security practices. Key measures include enabling two-factor authentication, installing antivirus software, and verifying suspicious messages.

Future research should explore other influencing factors, such as education, work background, and exposure to digital training. These variables may explain why certain groups adopt stronger protective behaviors than others. In addition, future research should ensure data normality, which would allow the use of parametric tests such as one-way ANOVA and strengthen the robustness of statistical comparisons.

ACKNOWLEDGEMENT

This research was supported by the Directorate of Research and Community Service, Directorate General of Research and Development, Ministry of Higher Education, Science, and Technology, and LPPM Universitas Syiah Kuala under Sub-Contract Number: 92/UN11.L1/PG.01.03/DPPM/2025.

REFERENCES

- Adeoye, O. (2012). Evaluating the performance of a two-factor authentication solution in the banking sector. *International Journal of Computer Science Issues*, 9.
- Agrawal, D., Singh, K., & Sharma, D. (2025). Understanding Gen Z's vulnerability to romance scams.
- Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of COVID-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10, Part A), 8176-8206. <https://doi.org/https://doi.org/10.1016/j.jksuci.2022.08.003>
- Antara News Aceh. (2025). *OJK ungkap 1.987 laporan penipuan keuangan ilegal di Aceh*. https://aceh.antaranews.com/berita/387769/ojk-ungkap-1987-laporan-penipuan-keuangan-ilegal-di-aceh?utm_source=chatgpt.com
- Çoklar, A. N., & Tatli, A. (2021). Examining the digital nativity levels of digital generations: From generation X to generation Z. *Shanlax International Journal of Education*, 9(4), 433-444.
- Debb, S., Schaffer, D., & Colson, D. (2020). A reverse digital divide: Comparing information security behaviors of generation Y and generation Z adults. *The International Journal of Cybersecurity Intelligence and Cybercrime*, 3, 42-55. <https://doi.org/10.52306/03010420GXUV5876>
- Dinas Komunikasi dan Informatika Kabupaten Sleman. (2022). *Mengukur tingkat literasi digital masyarakat Kabupaten Sleman*. <https://kominfo.slemankab.go.id/wp-content/uploads/2023/08/Mengukur-Tingkat-Literasi-Digital-Masyarakat-kab.-Sleman-2022-ebook.pdf>
- Farhani, M. T., & Isnawati, M. (2023). Pertanggungjawaban pidana pelaku tindak pidana penipuan belanja daring dalam metode pembayaran ditempat. *ACADEMOS Jurnal Hukum dan Tatahan Sosial*, 2(1).
- Golzar, J., Noor, S., & Tajik, O. (2022). Convenience sampling. *International Journal of Education & Language Studies*, 1(2), 72-77. <https://doi.org/10.22034/ijels.2022.162981>
- Hikmah, B., Muaz, R., & Rachman, I. (2024). Program gerakan nasional literasi digital (GNLD): Upaya pemerintah Indonesia dalam mewujudkan sustainable development goals (SDGs) 2030. *Jurnal Nakula : Pusat Ilmu Pendidikan, Bahasa dan Ilmu Sosial*, 2, 253-265. <https://doi.org/10.61132/nakula.v2i3.825>
- Jiang, M., Tsai, H.-y. S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, 42(9), 621-634. <https://doi.org/10.1080/03601277.2016.1205408>

- Jovanović, I., Cvjetkovic, M., & Cvjetković, M. (2024). The impact of the application of antivirus programs on the security of computer systems. *Bizinfo Blace*, 15, 11-19. <https://doi.org/10.5937/bizinfo2402011J>
- Kamran, M., & Maskun, M. (2021). Penipuan dalam jual beli online: Perspektif hukum telematika [Positive Law; Online Buying and Selling; Fraud]. 2021, 1(1), 16. <https://doi.org/10.47268/balobe.v1i1.501>
- Kominfo, & Katadata Insight Center. *Status literasi digital di Indonesia 2022*. <https://cdn1.katadata.co.id/media/microsites/litdik/ReportSurveiStatusLiterasiDigitalIndonesia2022.pdf>
- Kurnia, N., Rahayu, Wendratama, E., Monggilo, Z. M. Z., Damayanti, A., Angendari, D. A. D., Abisono, F. Q. a., Shafira, I., & Desmalinda. (2022). *Penipuan digital di Indonesia: Modus, medium, dan rekomendasi*. Program Studi Magister Ilmu Komunikasi Fakultas Ilmu Sosial dan Ilmu Politik Universitas Gadjah Mada.
- Li, P., Li, Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. *International Review of Economics & Finance*, 91, 364-377. <https://doi.org/https://doi.org/10.1016/j.iref.2024.01.056>
- Long, T. Q., Hoang, T. C., & Simkins, B. (2023). Gender gap in digital literacy across generations: Evidence from Indonesia. *Finance Research Letters*, 58, 104588. <https://doi.org/https://doi.org/10.1016/j.frl.2023.104588>
- Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, 62(10), 1356-1371. <https://doi.org/10.1177/0002764218787854>
- Nisa, U., Nisak, C. L. C., & Fatia, D. (2023). Literasi digital lansia pada aspek digital skill dan digital safety [Digital Literacy; Digital Safety; Digital Skill; Elderly; Lansia; Literasi Digital]. 2023, 12(1), 25. <https://doi.org/10.24815/jkg.v12i1.31667>
- Ostertagová, E., Ostertag, O., & Kováč, J. (2014). Methodology and application of the kruskal-wallis test. *Applied Mechanics and Materials*, 611, 115-120. <https://doi.org/10.4028/www.scientific.net/AMM.611.115>
- Puram, P., Kaparathi, M., Krishna, A., & Rayaprolu, H. (2011). Online scams: Taking the fun out of the internet. *Indian Journal of Computer Science and Engineering*, 2.
- Puspitasari, I. (2018). Pertanggungjawaban pidana pelaku tindak pidana penipuan online dalam hukum positif di Indonesia. *Humani (Hukum dan Masyarakat Madani)*, 8(1), 1-14.
- Putra, Y. S. (2017). Theoretical review: Teori perbedaan generasi. *Among Makarti*, 9. <https://doi.org/10.52353/ama.v9i2.142>
- Rahmad, N. (2019). Kajian hukum terhadap tindak pidana penipuan secara online. *Jurnal Hukum Ekonomi Syariah*, 3(2), 103-117.

- Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security*, 136, 103558. <https://doi.org/https://doi.org/10.1016/j.cose.2023.103558>
- Robinson, L., Schulz, J., Dunn, H. S., Casilli, A. A., Tubaro, P., Carvath, R., Chen, W., Wiest, J. B., Dodel, M., & Stern, M. J. (2020). Digital inequalities 3.0: Emergent inequalities in the information age. *First Monday*, 25(7).
- Rowe, B., Halpern, M., Lentz, T., & Wood, D. (2012). Understanding cyber security risk preferences: A case study analysis inspired by public health research. *Institute for Homeland Security Solutions*.
- Sanjaya, S., Fitriati, L. R., Hakim, M. A., Yasin, M. Y., & Maesarah, S. S. (2024). Analisis literasi keamanan digital bagi mahasiswa universitas tasikmalaya: Tingkat pengetahuan, kepercayaan, dan kewaspadaan. *Innovative: Journal Of Social Science Research*, 4(3), 8205-8216.
- Saputra, D. F. (2023). Literasi digital untuk perlindungan data pribadi. *Jurnal Ilmu Kepolisian*, 17(3).
- Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *J Elder Abuse Negl*, 31(3), 225-243. <https://doi.org/10.1080/08946566.2019.1625842>
- Syam, H. M., & Nurrahmi, F. (2020). "I don't know if it is fake or real news": How little Indonesian university students understand social media literacy. *Jurnal Komunikasi: Malaysian Journal of Communication*, 36(2), 92-105.
- The Aceh Post. (2025). *OJK Aceh Catat 84 Laporan Aktivitas Keuangan Ilegal Selama Juni 2025*. https://theacehpost.com/news/ojk-aceh-catat-84-laporan-aktivitas-keuangan-ilegal-selama-juni-2025/index.html?utm_source=chatgpt.com
- Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138-150. <https://doi.org/https://doi.org/10.1016/j.cose.2016.02.009>
- van 't Hoff-de Goede, M. S., Leukfeldt, E. R., van de Weijer, S. G. A., & van der Kleij, R. (2025). Does protection motivation predict self-protective online behaviour? Comparing self-reported and actual online behaviour using a population-based survey experiment. *Computers in Human Behavior Reports*, 18, 100649. <https://doi.org/https://doi.org/10.1016/j.chbr.2025.100649>
- Wongmahesak, K., Singh, B., & Kaunert, C. (2025). The complex interplay of generational differences, digital literacy, and cybercrime fear is a significant factor. *Asian Crime and Society Review*, 12(1), Article 3. <https://doi.org/10.14456/acsr.2025.3>