



International Journal of Agriculture Extension and Social Development

ISSN Print: 2618-0723
ISSN Online: 2618-0731
NAAS Rating (2026): 5.04
IJAESD 2026; 9(10): 392-398
www.extensionjournal.com
Received: 14-08-2026
Accepted: 30-09-2026
Published: 10-10-2026

The names and affiliations of all authors are provided below, following the references.

Corresponding Author: Charvi Mehra

IM.Sc. Research Scholar,
RMCS Department CCAS,
MPUAT, Udaipur, 2Former
Emeritus Professor, RMCS
Department CCAS, MPUAT,
Udaipur, 3Professor, RMCS
Department CCAS, MPUAT,
Udaipur, 4Assistant
Professor, HDFS
Department CCAS, MPUAT,
Udaipur, 5Assistant
Professor, EECM
Department CCAS, MPUAT,
Udaipur, Rajasthan, India

Assessment on awareness of cyber threats and cyber security among middle-aged and elderly population

Charvi Mehra¹, Rekha Vyas², Hemu Rathore³, Monika Rai⁴, Vishaka Bansal M.Sc. Research Scholar⁵

DOI: <https://www.doi.org/10.33545/26180723.2026.v9.i10f.4408>

ABSTRACT

This exploratory study assessed awareness of cyber threats and cyber security among 120 middle-aged (40–59 years) and elderly (60–70 years) persons in Udaipur city, Rajasthan, with equal numbers of males and females in each age group. Respondents were selected by snowball sampling, and data were collected through a structured questionnaire administered in face-to-face interviews. Smartphones and digital payment platforms were used by almost all respondents, and 97.5% had experienced some form of cyber threat, most often through phone calls (82.5%). Familiarity with the terms "cyber threats" (38.3%) and "cyber security" (50.0%) was low. Respondents knew common frauds such as phishing, online banking fraud and OTP fraud, but technical safeguards such as two-factor authentication, software updates and antivirus use were poorly known and adopted. Only 14.2% knew how to report a cybercrime, and 40.0% were aware of government initiatives. Middle-aged respondents had significantly better knowledge of threats and safe practices, whereas the elderly were more cautious about checking website security and avoiding unknown QR codes. Gender differences were item-specific and not consistent in direction. Notably, 84.2% of respondents were willing to attend an awareness programme. The findings point to the need for simple, repeated, age-appropriate cyber security education in the local language, with clear guidance on reporting.

Keywords: Cyber threats, Cyber security awareness, Middle-aged, Elderly, Digital payments, Cybercrime reporting

Introduction

Digital technologies have become an inseparable part of everyday life. Smartphones, messaging applications, social media, online banking, digital payment systems, e-commerce and government e-services are now used by people of almost all age groups for communication, financial transactions, shopping and access to information. While these developments have brought convenience, speed and accessibility, they have also increased individuals' exposure to cyber threats such as phishing, online financial fraud, identity theft, social engineering and malicious applications.

Cyber security is not solely a technical matter. Many cyber incidents succeed because users are deceived or pressured into acting against their own interest, for example by sharing one-time passwords (OTPs), clicking on fraudulent links or trusting callers who impersonate officials. Studies of deceptive messages have shown that the content and framing of a message, including appeals to urgency and authority, influence how recipients respond (Oliveira *et al.*, 2017) [1]. Cyber security awareness therefore involves both knowledge of threats and the ability to adopt appropriate protective behavior, and awareness alone does not always translate into safe practice because information-based campaigns often fail to build safe habits (Bada *et al.*, 2019) [2].

Middle-aged and elderly persons form an important group in this context. They increasingly use digital banking, payment applications and messaging services, yet they differ from younger users in prior technological experience, confidence and access to support. Research in ageing has linked older age with poorer discrimination between genuine and phishing emails (Grilli *et al.*, 2021) [3] and greater phishing susceptibility (Pehlivanoglu *et al.*, 2024) [4], and has shown that education, prior awareness and cognitive and socio-emotional resources influence the ability to recognise deception (Gavett *et al.*, 2017; Ebner *et al.*, 2020) [6, 5]. At the same time, other work cautions that older adults should not be treated as a homogeneous or automatically more vulnerable group (Ross *et al.*, 2014; Shang *et al.*, 2022) [7, 8]. Older adults often regard protective behaviour as important but hesitate to adopt it because of perceived effort, fear of making mistakes and lack of accessible guidance (Morrison *et al.*, 2021) [9].

In India, rapid digitalisation and the widespread use of the Unified Payments Interface (UPI) have been accompanied by growing reports of cyber fraud, including impersonation calls, fake KYC and OTP messages, QR-code scams and fraudulent investment offers. The national cybercrime helpline 1930 and the National Cyber Crime Reporting Portal have been introduced to help victims report such incidents promptly, and

agencies such as CERT-In conduct awareness activities. Whether ordinary users know about and use these mechanisms is, however, an empirical question.

Much of the available research has been conducted in Western countries, many studies concentrate only on adults above 60 years, and relatively few examine awareness, experience of threats, safe practices and reporting knowledge together within the same population. Indian studies on the subject are limited (Sebastian *et al.*, 2022) [10]. Middle-aged adults, who are active users of digital banking and social media, have received comparatively less attention than the elderly. Therefore, the present study was undertaken with the following objectives: (i) to assess the awareness of middle-aged and elderly persons regarding cyber threats and cyber security, and (ii) to identify the cyber threats they encounter and to explore their online behaviour and safe digital practices, with a view to suggesting guidelines for safer digital participation.

Methodology

The study was exploratory and was conducted in Udaipur city, Rajasthan. With increasing digital use across age groups and feasibility of data collection. A total of 120 respondents were selected, comprising 60 middle-aged persons (40–59 years) and 60 elderly persons (60–70 years), with 30 males and 30 females in each age group. Respondents were identified through non-probability snowball sampling, in which initial respondents meeting the criteria referred to other eligible persons from their social network. Persons who actively used digital devices (smartphone, laptop, desktop, tablet or internet-enabled keypad phone) for activities such as communication, online financial transactions, shopping or social media, and who were willing to participate, were included.

Primary data were collected through a structured questionnaire developed in line with the objectives of the study. It had three sections: (I) socio-demographic and digital usage profile, including devices, platforms and security features used; (II) awareness and knowledge of cyber threats, cyber security practices and cybercrime reporting; and (III) behavioural practices, response to cyber fraud, awareness of government initiatives and willingness to attend awareness programmes.

Data were collected personally by the researcher through face-to-face interviews, after obtaining informed consent and assuring confidentiality and anonymity.

The data were then coded, tabulated and analysed using Microsoft Excel and the Statistical Package for the Social Sciences (SPSS). Frequency and percentage were used to describe the profile, awareness and practices of the respondents. The Pearson chi-square test of association (with Fisher's exact test for 2×2 tables) was used to compare middle-aged and elderly respondents, and male and female respondents within each age group, at the 0.05 level of significance.

Result and Discussion

Socio-demographic profile of respondents

The sample was equally divided by design between middle-aged and elderly respondents and between males and females. Table 1 shows that graduates formed the largest educational group (50.8%), followed by senior secondary (35.0%) and postgraduate (10.8%) respondents, and that no respondent was illiterate or had only primary education. Middle-aged respondents were significantly better educated than elderly respondents (63.3% graduates and 15.0% postgraduates versus 38.3% and 6.7%), while 48.3% of elderly respondents had studied only up to senior secondary level ($\chi^2 = 15.707$, $p = 0.001$). The upper-middle income group was the largest (56.7%), but a higher proportion of elderly respondents belonged to the higher income group (35.0% versus 11.7%; $\chi^2 = 9.284$, $p = 0.010$), which may reflect pensions and accumulated assets.

Occupation also differed significantly by age group ($\chi^2 = 29.958$, $p < 0.001$): 38.3% of middle-aged respondents were in government service, whereas 28.3% of elderly respondents were retired and 30.0% were homemakers. Most respondents (78.3%) lived in urban areas and 17.5% in semi-urban areas, with no rural respondents, and family type (nuclear 36.7%, extended 35.8%, joint 27.5%) and area of residence did not differ significantly between the age groups ($p > 0.05$). The sample was thus largely urban and educated, which should be kept in mind while interpreting the awareness levels reported below, since education and prior awareness have been found to help people recognise phishing (Gavett *et al.*, 2017) [6].

Table 1. Socio-demographic profile of middle-aged and elderly respondents.

Variable	Middle-aged (<i>n</i> = 60)	Elderly (<i>n</i> = 60)	Total (<i>n</i> = 120)	χ^2	<i>p</i> -value
Education qualification ($\chi^2 = 15.707$, <i>df</i> = 3)					
Secondary	0 (0.0)	4 (6.7)	4 (3.3)	15.707	0.001*
Senior secondary	13 (21.7)	29 (48.3)	42 (35.0)		
Graduate	38 (63.3)	23 (38.3)	61 (50.8)		
Postgraduate	9 (15.0)	4 (6.7)	13 (10.8)		
Income group ($\chi^2 = 9.284$, <i>df</i> = 2)					
Lower middle	13 (21.7)	11 (18.3)	24 (20.0)	9.284	0.010*
Upper middle	40 (66.7)	28 (46.7)	68 (56.7)		
Higher	7 (11.7)	21 (35.0)	28 (23.3)		

*Percentage in parenthesis

*Significant at $p < 0.05$; NS = Not significant

Digital exposure and security of devices

Table 2 shows that smartphones were used by all 120 respondents, and messaging (93.3%) and digital payment platforms (95.8%) were the most widely used, so both groups are routinely exposed to payment and OTP-related fraud. Computers were used by 51.7% of middle-aged respondents but by none of the elderly, who relied more on keypad phones (40.0% versus 20.0%). Middle-aged respondents had longer experience of digital devices (more than 10 years: 20.0% versus 8.3%; $\chi^2 = 11.482$, $p = 0.009$), whereas only elderly respondents (11.7%) had used devices for just 1–3 years. Almost all middle-aged respondents (98.3%) managed their devices themselves, compared with 75.0% of the elderly, who depended more on relatives (71.7%

versus 50.0%); no respondent reported having no source of help. Dependence on others can be a risk when passwords or OTPs are shared with the person helping. Social media use was also higher among middle-aged respondents (71.7% versus 51.7%).

Although 81.7% of respondents in both age groups considered their devices safe, the adoption of security features was limited. Password/PIN lock (80.0% versus 40.0%), two-factor authentication (55.0% versus 28.3%), privacy settings on apps (43.3% versus 21.7%) and regular software updates (35.0% versus 18.3%) were used significantly more by middle-aged respondents; the difference for software updates was marginal on Fisher's exact test ($p = 0.062$). Antivirus software was used by only 8.3% of respondents, with no

age difference, and 18.3% of elderly respondents used no security feature at all (6.7% of middle-aged; $p = 0.053$). The gap between perceived safety and the safeguards actually in use suggests that confidence in device safety may not rest on protective measures, a pattern

consistent with the observation that older adults' attitudes to protective behaviour are shaped by perceived effort and confidence rather than by knowledge alone (Morrison *et al.*, 2021) [9].

Table 2. Digital exposure and security features used by middle-aged and elderly respondents.

Variable	Middle-aged ($n = 60$)	Elderly ($n = 60$)	Total ($N = 120$)	χ^2	p -value
Devices, experience and assistance					
Computer / PC	31 (51.7)	0 (0.0)	31 (25.8)	41.798	< 0.001*
Keypad phone	12 (20.0)	24 (40.0)	36 (30.0)	5.714	0.017*
Manages device on own (self)	59 (98.3)	45 (75.0)	104 (86.7)	14.135	< 0.001*
Takes help from relatives	30 (50.0)	43 (71.7)	73 (60.8)	5.911	0.015*
Digital platforms used					
Messaging / communication	60 (100.0)	52 (86.7)	112 (93.3)	8.571	0.003*
Social media	43 (71.7)	31 (51.7)	74 (61.7)	5.076	0.024*
Digital payment	58 (96.7)	57 (95.0)	115 (95.8)	0.209	0.648 NS
Security features used on devices					
Password / PIN lock	48 (80.0)	24 (40.0)	72 (60.0)	20.000	< 0.001*
Two-factor authentication	33 (55.0)	17 (28.3)	50 (41.7)	8.777	0.003*
Privacy settings on apps	26 (43.3)	13 (21.7)	39 (32.5)	6.420	0.011*
Regular software updates	21 (35.0)	11 (18.3)	32 (26.7)	4.261	0.039*
Fingerprint lock	29 (48.3)	21 (35.0)	50 (41.7)	2.194	0.139 NS
Antivirus software	6 (10.0)	4 (6.7)	10 (8.3)	0.436	0.509 NS
No security feature	4 (6.7)	11 (18.3)	15 (12.5)	3.733	0.053 NS
Perception of device safety					
Considers device safe	49 (81.7)	49 (81.7)	98 (81.7)	0.000	1.000 NS

*Percentage in parenthesis

*Significant at $p < 0.05$; NS = Not significant. Devices, platforms and security features were multiple-response items.

Awareness of cyber threats

Table 3 shows that familiarity with the terms themselves was low: only 38.3% of respondents had heard of “cyber threats” (48.3% were not sure) and 50.0% had heard of “cyber security”, with no significant difference between the age groups. Yet 97.5% had experienced some form of cyber threat, and phone calls were by far the most common channel (82.5%), reported more by middle-aged respondents (96.7% versus 68.3%; $\chi^2 = 16.681$, $p < 0.001$), followed by messaging apps (53.3%) and SMS (48.3%). Respondents therefore seem to recognise fraud through experience rather than through technical terminology. The predominance of phone calls also indicates that voice-based approaches, in which urgency and false authority can be applied directly, are an important route for fraud, in line with evidence that persuasive framing influences responses to deceptive messages (Oliveira *et al.*, 2017) [1].

Knowledge of specific threats was highest for phishing (81.7%), on-line banking fraud (79.2%) and OTP fraud (73.3%), and middle-aged respondents were significantly more knowledgeable than elderly respondents about all three (phishing 100.0% versus 63.3%; banking fraud 95.0% versus 63.3%; OTP fraud 86.7% versus 60.0%). Knowledge of card fraud, identity theft and online shopping fraud was similar in both groups, while technical threats such as malware (27.5%) and ransomware (20.8%) were poorly known by everyone. The greater difficulty of the elderly in recognising deceptive communication is consistent with earlier findings that older age is related to poorer discrimination between genuine and phishing messages (Grilli *et al.*, 2021; Pehlivanoglu *et al.*, 2024) [3, 4], although the similar levels for several threats show that the elderly are not uniformly less aware (Ross *et al.*, 2014; Shang *et al.*, 2022) [7, 8].

Table 3. Awareness and experience of cyber threats among middle-aged and elderly respondents.

Variable	Middle-aged ($n = 60$)	Elderly ($n = 60$)	Total ($n = 120$)	χ^2	p -value
Familiarity with terms					
Heard of the term “cyber threats” (Yes)	26 (43.3)	20 (33.3)	46 (38.3)	1.308	0.520 NS
Heard of the term “cyber security” (Yes)	29 (48.3)	31 (51.7)	60 (50.0)	3.590	0.166 NS
Ever experienced a cyber threat	58 (96.7)	59 (98.3)	117 (97.5)	0.342	0.559 NS
Knowledge of types of cyber threats					
Phishing	60 (100.0)	38 (63.3)	98 (81.7)	26.939	< 0.001*
Online banking fraud	57 (95.0)	38 (63.3)	95 (79.2)	18.240	< 0.001*
OTP fraud	52 (86.7)	36 (60.0)	88 (73.3)	10.909	0.001*
Credit / debit card fraud	40 (66.7)	39 (65.0)	79 (65.8)	0.037	0.847 NS
Online shopping fraud	35 (58.3)	35 (58.3)	70 (58.3)	0.000	1.000 NS
Identity theft	36 (60.0)	33 (55.0)	69 (57.5)	0.307	0.580 NS

(continued on next page)

Variable	Middle-aged (n = 60)	Elderly (n = 60)	Total (n = 120)	χ^2	p-value
Malware / virus attacks	14 (23.3)	19 (31.7)	33 (27.5)	1.045	0.307 NS
Ransomware attacks	10 (16.7)	15 (25.0)	25 (20.8)	1.263	0.261 NS
Channel through which most threats were received					
Phone calls	58 (96.7)	41 (68.3)	99 (82.5)	16.681	< 0.001*
Messaging apps	34 (56.7)	30 (50.0)	64 (53.3)	0.536	0.464 NS
SMS	31 (51.7)	27 (45.0)	58 (48.3)	0.534	0.465 NS

*Percentage in parenthesis*Significant at $p < 0.05$; NS = Not significant. Types of threats and channels were multiple-response items.

Knowledge of safe practices, reporting and government initiatives

As shown in Table 4, the best-known practices were not sharing passwords (66.7%) and creating strong passwords (65.8%), and middle-aged respondents knew both significantly better than the elderly (88.3% versus 45.0% and 85.0% versus 46.7%). Technical safeguards were poorly known in both groups, with no significant age difference: avoiding suspicious links (32.5%), regular software updates (27.5%), two-factor authentication (25.8%), logging out from public devices (25.8%) and antivirus software (17.5%). This low knowledge helps to explain the limited adoption of these measures seen in Table 2. A similar situation was reported among adults in Kerala, where awareness programmes and structured workshops were recommended to improve cyber practices (Sebastian *et al.*, 2022) [10].

Knowledge about reporting was a particular weakness. Only 14.2% of respondents knew how to report a cybercrime, 39.2% had heard of reporting but did not know the procedure and 45.0% were not aware of it at all. The elderly were considerably less informed, with 63.3% not aware compared with 26.7% of the middle-aged ($\chi^2 = 17.97$, $p < 0.001$). The local police station (80.8%) and friends or family (78.3%) were the best-known sources of help, whereas the national cybercrime portal was known to only 23.3% in both age groups and helpline 1930 to 51.7%. Awareness of collecting evidence was significantly lower among the elderly (23.3% versus 55.0%), and only 40.0% of respondents knew of government initiatives such as CERT-In and the National Cyber Security Policy (53.3% of the middle-aged versus 26.7% of the elderly; $\chi^2 = 8.889$, $p = 0.003$). These findings suggest that official channels have not reached the elderly effectively and that the traditional route of the local police station is better known than online reporting.

Table 4. Knowledge of safe practices, reporting procedures and government initiatives.

Variable	Middle-aged (n = 60)	Elderly (n = 60)	Total (N = 120)	χ^2	p-value
Knowledge of cyber security practices					
Creating strong passwords	51 (85.0)	28 (46.7)	79 (65.8)	19.599	< 0.001*
Not sharing passwords	53 (88.3)	27 (45.0)	80 (66.7)	25.350	< 0.001*
Avoiding suspicious links	21 (35.0)	18 (30.0)	39 (32.5)	0.342	0.559 NS
Two-factor authentication	20 (33.3)	11 (18.3)	31 (25.8)	3.523	0.061 NS
Regular software updates	19 (31.7)	14 (23.3)	33 (27.5)	1.045	0.307 NS
Logging out from public devices	18 (30.0)	13 (21.7)	31 (25.8)	1.087	0.297 NS
Using antivirus software	10 (16.7)	11 (18.3)	21 (17.5)	0.058	0.810 NS
Knowledge of how to report cyberthreats ($\chi^2 = 17.97$, $df = 2$, $p < 0.001$*)					
Yes, know the procedure	12 (20.0)	5 (8.3)	17 (14.2)		
Heard, but do not know the procedure	32 (53.3)	15 (25.0)	47 (39.2)		
Not aware	16 (26.7)	38 (63.3)	54 (45.0)	17.970	< 0.001*
Awareness of reporting platforms and government initiatives					
National cybercrime reporting portal	14 (23.3)	14 (23.3)	28 (23.3)	0.000	1.000 NS
Helpline number 1930	32 (53.3)	30 (50.0)	62 (51.7)	0.133	0.715 NS
Local police station	52 (86.7)	45 (75.0)	97 (80.8)	2.636	0.104 NS
Collecting evidence	33 (55.0)	14 (23.3)	47 (39.2)	12.626	< 0.001*
Friends / family members as source of help	56 (93.3)	38 (63.3)	94 (78.3)	15.908	< 0.001*
Aware of government initiatives (CERT-In, NCSP etc.)	32 (53.3)	16 (26.7)	48 (40.0)	8.889	0.003*

*Percentage in parenthesis

*Significant at $p < 0.05$; NS = Not significant. Practices and platforms were multiple-response items.

Safe digital practices and response to cyber fraud

Table 5 shows that several precautions during online payments were followed by most respondents: not sharing OTP, PIN or passwords (92.5%), using trusted payment applications (87.5%), verifying receiver details (84.2%) and checking transaction details (78.3%). Other precautions were less common, such as ensuring that the website or application is secure (40.8%) and regularly checking bank statements or alerts (52.5%). The age pattern was mixed rather than uniformly in

favour of the middle-aged: middle-aged respondents more often used trusted payment applications (95.0% versus 80.0%), while elderly respondents more often checked that the website or application was secure (53.3% versus 28.3%) and avoided unknown QR codes (86.7% versus 71.7%; Fisher's exact $p = 0.071$). Mixed age-related differences in security behaviour have also been reported by Branley-Bell *et al.* (2022) [11], who found that older adults were less likely to secure their devices but more likely to adopt some other protective behaviours.

For other digital activities, middle-aged respondents followed safer practices significantly more often: not sharing personal information (93.3% versus 65.0%), using strong and unique passwords (73.3% versus 53.3%), not sharing OTPs or passwords (80.0% versus 58.3%) and avoiding suspicious links (55.0% versus 33.3%). Antivirus installation (30.0%), avoiding unknown apps (40.8%) and logging out of shared devices (38.3%) were low in both groups. Only 15.0% checked their privacy settings regularly, 41.7% did so sometimes and 15.8% never did, with no significant age difference ($p = 0.095$). That respondents knew a practice but did not follow it consistently supports the view that awareness alone does not secure safe behaviour (Bada *et al.*, 2019) [2].

In case of cyber fraud, no respondent said they would ignore the incident. Seeking help from family members or technical experts

(91.7%), informing the bank (84.2%) and blocking the suspicious number or account (84.2%) were the most common first actions, while reporting to helpline 1930 (61.7%) and on the national portal (31.7%) were less common. Elderly respondents were less likely to turn first to family (85.0% versus 98.3%; $p = 0.008$) but more likely to report on the national portal (41.7% versus 21.7%; $p = 0.019$). A high proportion of respondents (84.2%) were willing to attend a cyber security awareness programme, with no difference between age groups (86.7% versus 81.7%; $p = 0.453$). This agrees with the finding that older adults want to protect themselves but need accessible guidance and continuing support (Morrison *et al.*, 2021) [9], and it offers a favourable basis for community-level education.

Table 5. Safe digital practices, response to cyber fraud and willingness to participate in awareness programmes.

Variable	Middle-aged ($n = 60$)	Elderly ($n = 60$)	Total ($N = 120$)	χ^2	p -value
Practices followed during online payments					
Use trusted / official payment app	57 (95.0)	48 (80.0)	105 (87.5)	6.171	0.013*
Not sharing OTP / PIN / password	58 (96.7)	53 (88.3)	111 (92.5)	3.003	0.083 NS
Ensure website / app is secure	17 (28.3)	32 (53.3)	49 (40.8)	7.761	0.005*
Not clicking unknown QR codes	43 (71.7)	52 (86.7)	95 (79.2)	4.093	0.043*
Regularly check bank statements / alerts	28 (46.7)	35 (58.3)	63 (52.5)	1.637	0.201 NS
Practices followed while using devices for other purposes					
Do not share personal information	56 (93.3)	39 (65.0)	95 (79.2)	14.602	< 0.001*
Use strong and unique passwords	44 (73.3)	32 (53.3)	76 (63.3)	5.167	0.023*
Do not share OTPs / passwords	48 (80.0)	35 (58.3)	83 (69.2)	6.604	0.010*
Avoid clicking suspicious links	33 (55.0)	20 (33.3)	53 (44.2)	5.711	0.017*
Install antivirus / security software	16 (26.7)	20 (33.3)	36 (30.0)	0.635	0.426 NS
First action in case of cyber fraud					
Seek help from family / technical experts	59 (98.3)	51 (85.0)	110 (91.7)	6.982	0.008*
Inform the bank	52 (86.7)	49 (81.7)	101 (84.2)	0.563	0.453 NS
Report to helpline 1930	39 (65.0)	35 (58.3)	74 (61.7)	0.564	0.453 NS
Report on national cybercrime portal	13 (21.7)	25 (41.7)	38 (31.7)	5.546	0.019*
Willingness to participate in awareness programme					
Yes	52 (86.7)	49 (81.7)	101 (84.2)	0.563	0.453 NS

*Percentage in parenthesis

*Significant at $p < 0.05$; NS = Not significant. Practices and actions were multiple-response items.

Gender-wise differences within age groups

Table 6 presents the items on which male and female respondents differed significantly within each age group; on the remaining items no significant gender difference was found. Among middle-aged respondents, females were more aware of online shopping fraud (86.7% versus 30.0%) and all of them knew about creating strong passwords (100.0% versus 70.0%), but males more often reported protective behaviour: avoiding suspicious links (76.7% versus 33.3%), enabling privacy settings (93.3% versus 40.0%) and regularly checking bank statements (66.7% versus 26.7%). Middle-aged males were also more likely to consider their devices safe (93.3% versus 70.0%) and to know of government initiatives (66.7% versus 40.0%), although the latter was borderline on Fisher's exact test ($p = 0.069$).

Among elderly respondents the pattern differed. Elderly females were more likely to know about two-factor authentication (30.0% versus 6.7%) and software updates (40.0% versus 6.7%), to be aware of call and message verification apps (93.3% versus 53.3%) and to enable privacy settings (83.3% versus 46.7%), but 33.3% of them had not heard of the term cyber security, against 6.7% of elderly males ($p = 0.016$). Elderly males relied more on government campaigns for information (80.0% versus 43.3%). Gender differences were therefore item-specific and ran in different directions in the two age groups, rather than showing one gender to be consistently more aware. This is in keeping with Branley-Bell *et al.* (2022) [11], who found that gender did not directly predict cyber security behaviour.

Table 6. Significant gender-wise differences within middle-aged and elderly respondents.

Variable	Male ($n = 30$)	Female ($n = 30$)	χ^2	p -value
Middle-aged respondents				
Knows online shopping fraud	9 (30.0)	26 (86.7)	19.817	< 0.001*
Knows creating strong passwords	21 (70.0)	30 (100.0)	10.588	0.001*
Considers device safe	28 (93.3)	21 (70.0)	5.455	0.020*

(continued on next page)

Variable	Male (n = 30)	Female (n = 30)	χ^2	p-value
Avoids clicking suspicious links	23 (76.7)	10 (33.3)	11.380	0.001*
Enables privacy settings	28 (93.3)	12 (40.0)	19.200	< 0.001*
Regularly checks bank statements	20 (66.7)	8 (26.7)	9.643	0.002*
Aware of government initiatives	20 (66.7)	12 (40.0)	4.286	0.038*
Elderly respondents				
Has not heard of “cyber security” (No)	2 (6.7)	10 (33.3)	8.248	0.016*
Knows two-factor authentication	2 (6.7)	9 (30.0)	5.455	0.020*
Knows regular software updates	2 (6.7)	12 (40.0)	9.317	0.002*
Aware of call / message verification apps	16 (53.3)	28 (93.3)	12.273	< 0.001*
Enables privacy settings	14 (46.7)	25 (83.3)	8.864	0.003*
Learns about policies from government campaigns	24 (80.0)	13 (43.3)	8.531	0.003*

*Percentage in parenthesis

*Significant at $p < 0.05$. Only items with a significant difference are shown.

Conclusion

The study examined awareness of cyber threats and cyber security among 120 middle-aged and elderly persons in Udaipur city. Smartphones and digital payment platforms were used by almost all respondents, and nearly all (97.5%) had experienced some form of cyber threat, mainly through phone calls. Respondents knew common frauds such as phishing, online banking fraud and OTP fraud and a few basic practices such as not sharing passwords, but familiarity with the terms cyber threats and cyber security, knowledge of technical safeguards and use of antivirus software, two-factor authentication, software updates and privacy settings were low. Only 14.2% knew how to report a cyber threats and 40.0% were aware of government initiatives, although 84.2% were willing to attend awareness programmes.

Middle-aged respondents generally had better knowledge of threats and practices, used more security features and were better informed about reporting and government initiatives than the elderly, while the elderly depended more on others for operating devices. The age differences were not uniform: for example, elderly respondents were more careful about checking website security and unknown QR codes, and gender differences within each age group were item-specific. These findings point to the need for simple, practical and repeated cyber security education suited to each age group, delivered in the local language through demonstrations and realistic examples, with clear step-by-step guidance on reporting (informing the bank, calling helpline 1930, using the national cybercrime portal and preserving evidence) and with the involvement of family members, banks, educational institutions and the police. The findings should be read with caution because the sample was small, urban, relatively well educated and drawn by snowball sampling, and many comparisons were made, so isolated significant results may be due to chance.

References

- Oliveira D, Rocha H, Yang H, Ellis D, Dommaraju S, Muradoglu M, Weir D, Soliman A, Lin T, Ebner NC. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM. 2017:6412–6424.
- Bada M, Sasse AM, Nurse JRC. Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. 2019.
- Grilli MD, McVeigh KS, Hakim ZM, Wank AA, Getz SJ, Levin BE, Ebner NC, Wilson RC. Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails. The Journals of Gerontology: Series B. 2021;76(9):1711–1721.
- Pehlivanoglu D, Shoenfelt A, Hakim Z, Heemskerk A, Zhen J, Mosqueda M, Wilson RC, Huentelman M, Grilli MD, Turner G, Spreng RN, Ebner NC. Phishing vulnerability compounded by older age, apolipoprotein E e4 genotype, and lower cognition. PNAS Nexus. 2024;3(8):pgae296.
- Ebner NC, Ellis DM, Lin T, Rocha HA, Yang H, Dommaraju S, Soliman A, Woodard DL, Turner GR, Spreng RN, Oliveira DS. Uncovering susceptibility risk to online deception in aging. The Journals of Gerontology: Series B. 2020;75(3):522–533.
- Gavett BE, Zhao R, John SE, Bussell CA, Roberts JR, Yue C. Phishing suspiciousness in older and younger adults: The role of executive functioning. PLOS ONE. 2017;12(2):e0171620.
- Ross M, Grossmann I, Schryer E. Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. Perspectives on Psychological Science. 2014;9(4):427–442.
- Shang Y, Wu Z, Du X, Jiang Y, Ma B, Chi M. The psychology of the Internet fraud victimization of older adults: A systematic review. Frontiers in Psychology. 2022;13:912242.
- Morrison B, Coventry L, Briggs P. How do older adults feel about engaging with cyber-security? Human Behavior and Emerging Technologies. 2021;3(5):1033–1049.
- Sebastian SR, Babu BP. Are we cyber aware? A cross-sectional study on the prevailing cyber practices among adults from Thiruvalla, Kerala. International Journal of Community Medicine and Public Health. 2022;9(12).
- Branley-Bell D, Coventry L, Dixon M, Joinson A, Briggs P. Exploring age and gender differences in ICT cyber security behaviour. Human Behavior and Emerging Technologies. 2022;2022:2693080.

How to cite this article: Mehra C, Vyas R, Rathore H, Rai M, Scholar VBMSR. Assessment on awareness of cyber threats and cyber security among middle-aged and elderly population. *International Journal of Agriculture Extension and Social Development*. 2026;9(10):392-398. doi: <https://www.doi.org/10.33545/26180723.2026.v9.i10f.4408>

Authors

Charvi Mehra

1M.Sc. Research Scholar, RMCS Department CCAS, MPUAT, Udaipur, 2Former Emeritus Professor, RMCS Department CCAS, MPUAT, Udaipur, 3Professor, RMCS Department CCAS, MPUAT, Udaipur, 4Assistant Professor, HDFS Department CCAS, MPUAT, Udaipur, 5Assistant Professor, EECM Department CCAS, MPUAT, Udaipur, Rajasthan, India

Rekha Vyas

1M.Sc. Research Scholar, RMCS Department CCAS, MPUAT, Udaipur, 2Former Emeritus Professor, RMCS Department CCAS, MPUAT, Udaipur, 3Professor, RMCS Department CCAS, MPUAT, Udaipur, 4Assistant Professor, HDFS Department CCAS, MPUAT, Udaipur, 5Assistant Professor, EECM Department CCAS, MPUAT, Udaipur, Rajasthan, India

Hemu Rathore

1M.Sc. Research Scholar, RMCS Department CCAS, MPUAT, Udaipur, 2Former Emeritus Professor, RMCS Department CCAS, MPUAT, Udaipur, 3Professor, RMCS Department CCAS, MPUAT, Udaipur, 4Assistant Professor, HDFS Department CCAS, MPUAT, Udaipur, 5Assistant Professor, EECM Department CCAS, MPUAT, Udaipur, Rajasthan, India

Monika Rai

1M.Sc. Research Scholar, RMCS Department CCAS, MPUAT, Udaipur, 2Former Emeritus Professor, RMCS Department CCAS, MPUAT, Udaipur, 3Professor, RMCS Department CCAS, MPUAT, Udaipur, 4Assistant Professor, HDFS Department CCAS, MPUAT, Udaipur, 5Assistant Professor, EECM Department CCAS, MPUAT, Udaipur, Rajasthan, India

Vishaka Bansal M.Sc. Research Scholar

1M.Sc. Research Scholar, RMCS Department CCAS, MPUAT, Udaipur, 2Former Emeritus Professor, RMCS Department CCAS, MPUAT, Udaipur, 3Professor, RMCS Department CCAS, MPUAT, Udaipur, 4Assistant Professor, HDFS Department CCAS, MPUAT, Udaipur, 5Assistant Professor, EECM Department CCAS, MPUAT, Udaipur, Rajasthan, India