BruCERT Online Safety Awareness Survey 2025

CSB
CYBER SECURITY BRUNEI

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

Table of Contents

SECTION 1 – INTRODUCTION 3

Data Collection 4

Data Comparative Method 4

SECTION 2 – DEMOGRAPHIC PROFILE 5

Age Group 5

Employment & Educational Profile 6

SECTION 3 – DIGITAL HABITS 7

Digital Accessibility 7

SECTION 4 – ONLINE ACCOUNT SECURITY 10

Adoption & Perception 10

Perception of Social Media Information 11

Social Media Accessibility 13

Social Media Account Security Habits 14

E-mail Account Security Habits 15

SECTION 5 – PERSONAL EXPERIENCES 17

Identifying a Scam 22

SECTION 7 – ARTIFICIAL INTELLIGENCE (A.I.) 24

SECTION 8 – CONCLUSION 28

SECTION 1

Introduction

Brunei Computer Emergency Response Team (BruCERT) under Cyber Security Brunei (CSB) has conducted an online survey on Cybersecurity Awareness to assess the current level of understanding, attitudes and practices among the Bruneian population regarding online safety.

Respondents were given a series of questions covering these key focus areas:

1. Internet usage accessibility and habits.
2. Awareness of online risks.
3. Awareness of social media and online account risks.
4. Personal experience on cyber threats.
5. Awareness in Artificial Intelligence.

Survey Design

The survey consists of five main sections as mentioned above. Few questions were revised from past surveys with similar studies conducted back in 2022, which will serve as a benchmark for evaluating progress and emerging trends.

Distribution Method

The survey was distributed online, where a link was shared through social media accounts owned and managed by Cyber Security Brunei; BruCERT and csb.gov.bn. The link was promoted with an ‘incentive mechanic strategy’, where all respondents were given the choice to submit their details to enter into a lucky draw giveaway, where 3 of the total respondents will be selected at random

The survey was further promoted during two events between the duration of the research:

1. 26th August 2025; National Financial Literacy Day, STPRI Multipurpose Hall
2. 15th September 2025; Cyber Security Conference 2025 (CySec2025), The Rizqun Hotel

Data Collection

A total of 3,153 respondents were collected in the 3 week duration. The breakdown of the data collected are shown below:

Event - Programs - Links	Total Respondents
National Financial Literacy Day	971
Brunei Cybersecurity Conference 2025	977
Social Media	1019
Awareness Talks	186

Data Comparative Method

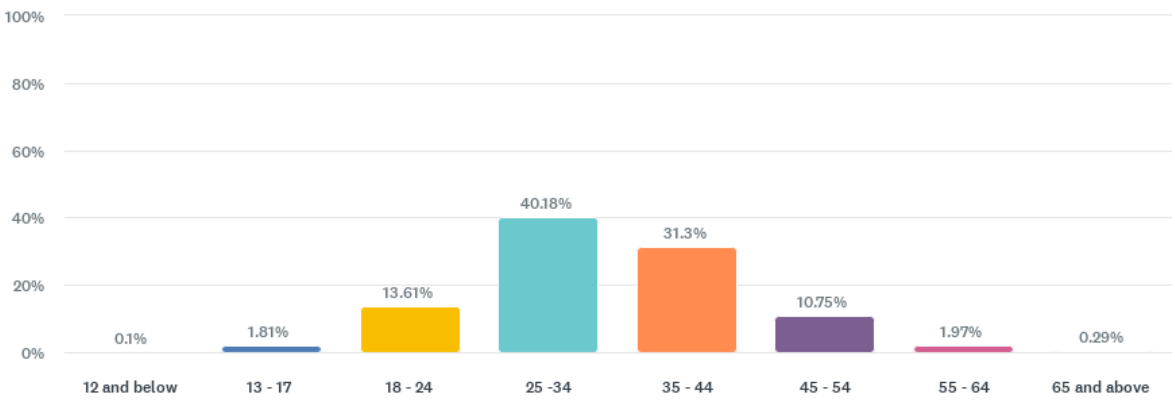
The analysis of the data collected for this report will be benchmarked with the earlier survey, conducted in 2022 (URL Link: Online Safety Survey 2022). The comparison may help understand the changes in digital habits and cyber security awareness.

SECTION 2

Demographic Profile

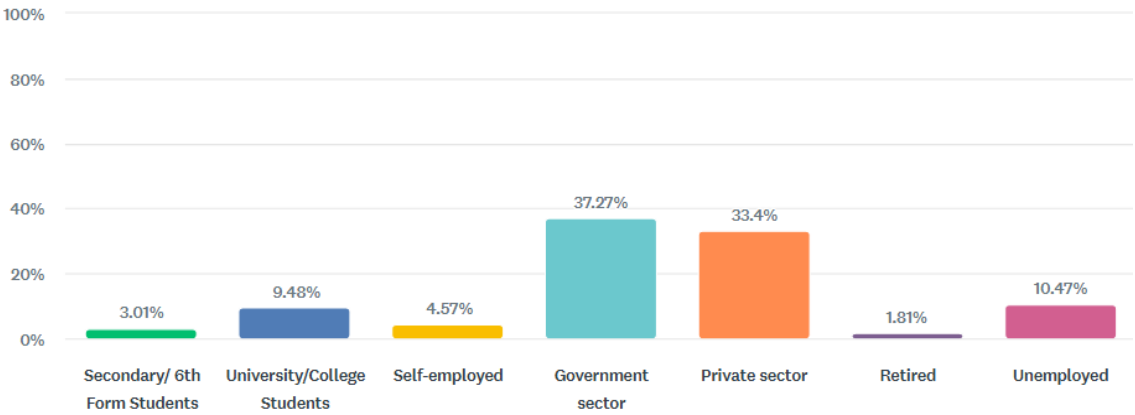
Age Group

The largest group of respondents for this survey is between the ages 25 to 34 years old (40.18%), following up with those between 35 to 44 years old, (31.30%).

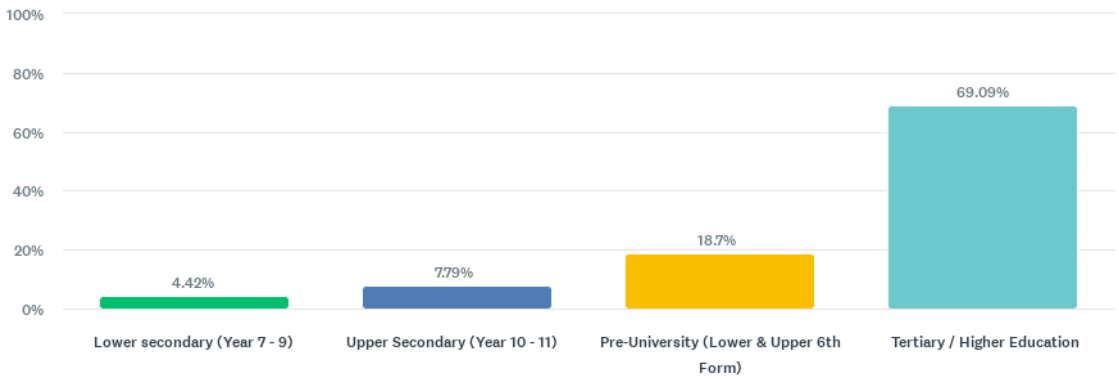


Employment & Educational Profile

A total of 75.24% of the respondents fall under the employed group, consisting of 37.27% from the government, 33.40% from the private sector and 4.57% are self-employed. The students and unemployed represent only 12.49% and 10.47% respectively.



Education Level



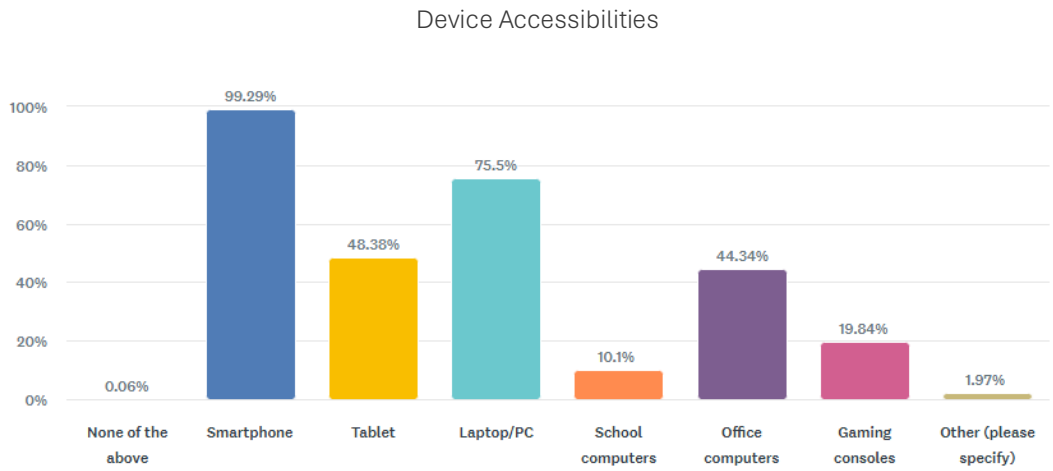
Among the 12.49% who are students, the majority are from Tertiary or higher education (69.09%), following up with Pre-university students (18.70%). Only a small fraction came from the upper secondary (7.79%) and lower secondary (4.42%).

SECTION 3

Digital Habits

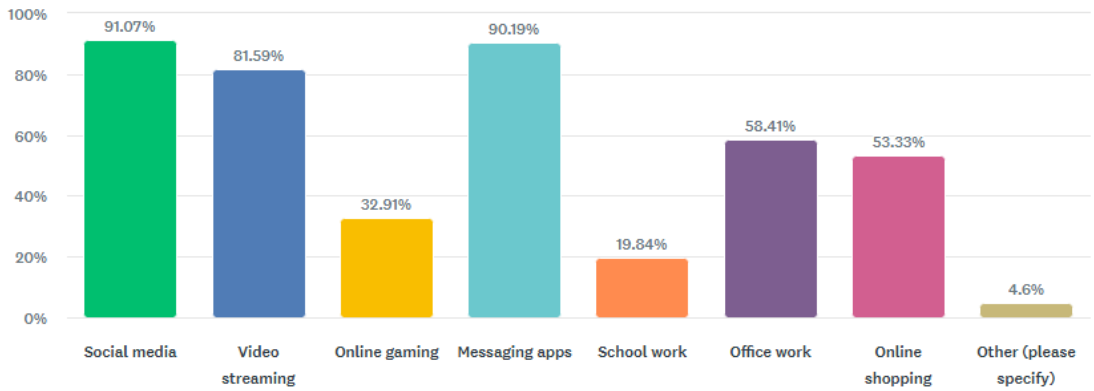
Digital Accessibility

Smartphones have the highest percentage (99.29%). The second highest accessible devices are laptops or PCs (75.50%). Followed up with tablets (48.38%) and work computers (44.34%).



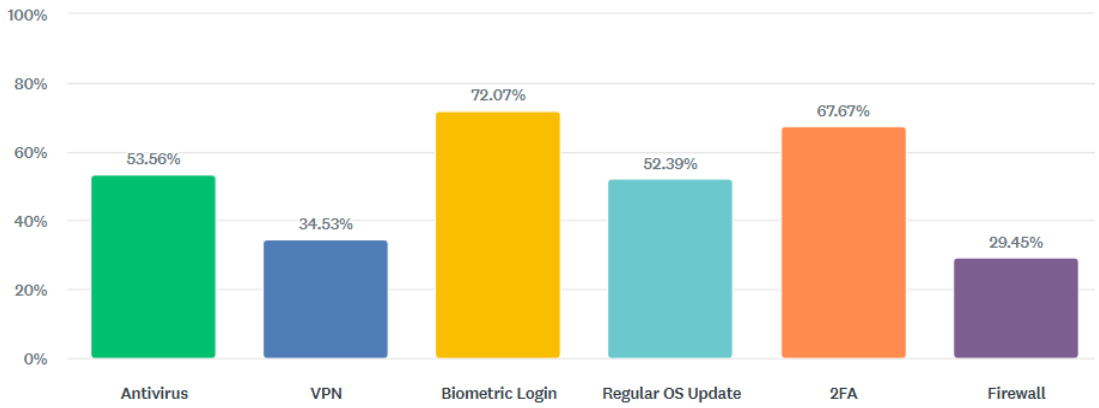
The top three activities reported are social media (91.07%), followed up by respondents using messaging applications (90.19%) such as WhatsApp and Telegram, as the third was reported video streaming (81.59%).

Online Activities

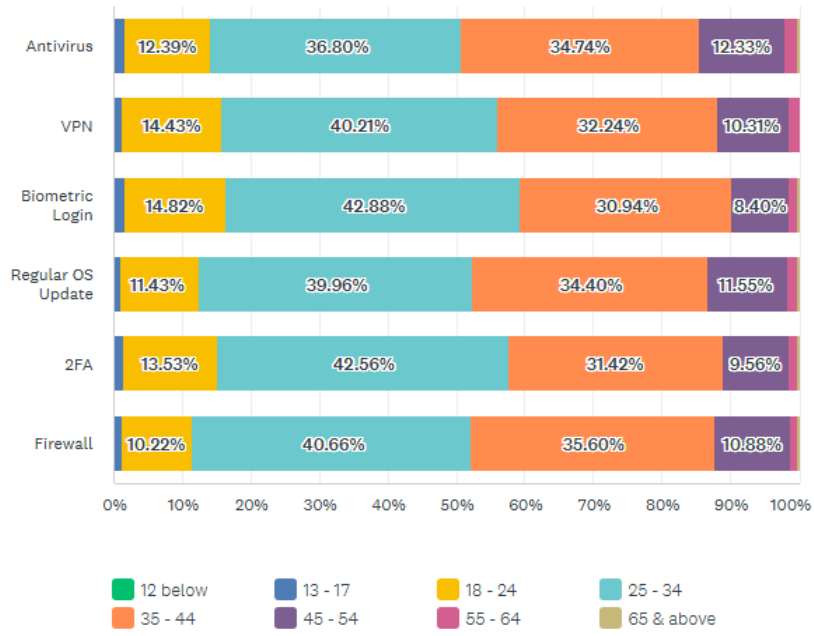


The top two security habits reported are biometric login (72.07%) and two-factor authentication (67.67%) respectively. 52.39% of the respondents were reported to keep their operating systems updated and 53.56% install antivirus software or applications.

Personal Security Habits



Personal Security Habits by Age



Personal security habits are concentrated among the working-age adults (25 - 34 and 35 - 44) with higher device usage and security awareness, with the use of biometric login (42.9%) and VPN (40.2%) application. Other age groups make up smaller shares which are below 15%.

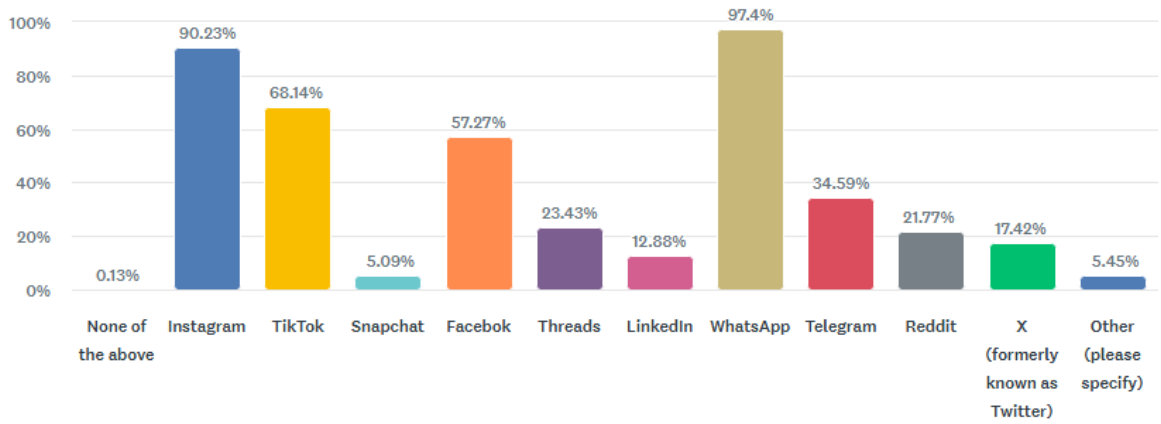
SECTION 4

Online Account Security

Adoption & Perception

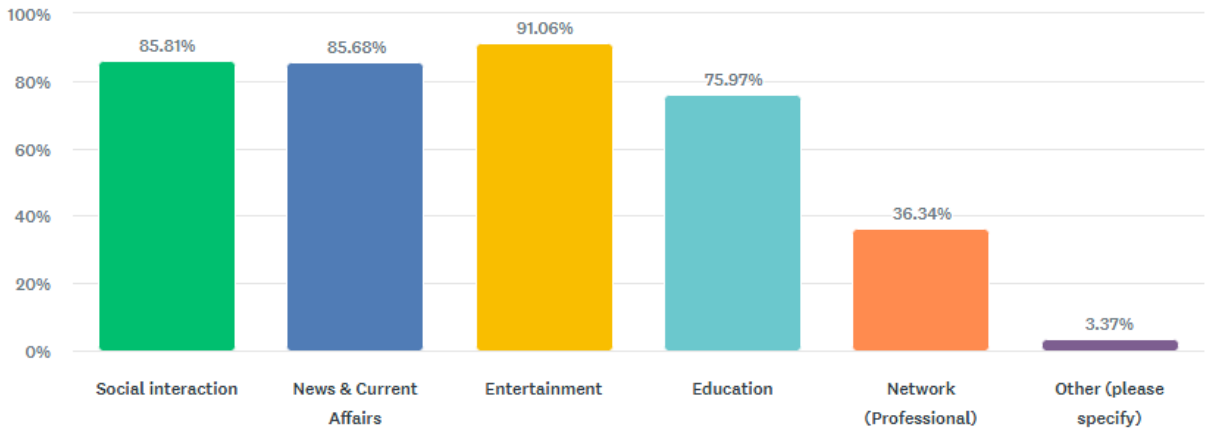
The most used online platforms are WhatsApp (97.40%) and Instagram (90.23%), followed by TikTok (68.14%) and Facebook (57.27%).

Which account platforms do you regularly use?



A total of 91.06% use their social platforms for entertainment purposes (videos, memes, music, etc). Closely followed by 'social interactions with friends and families (85.81%) and 'staying updated with news and current affairs' (85.68%).

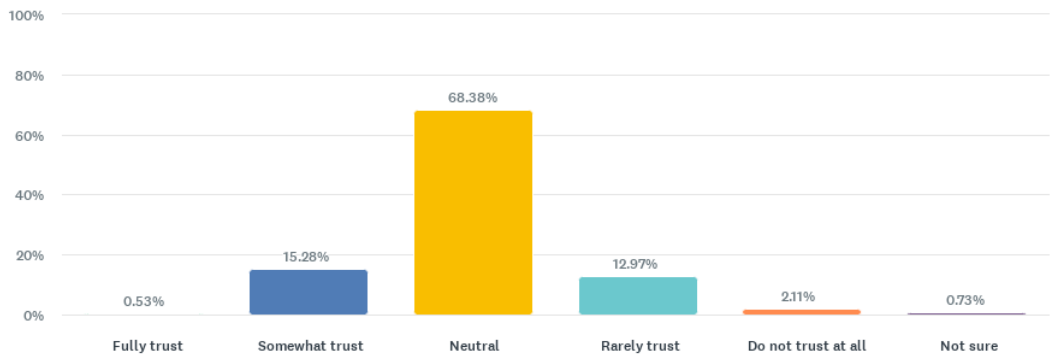
What is your purpose(s) of using social media?



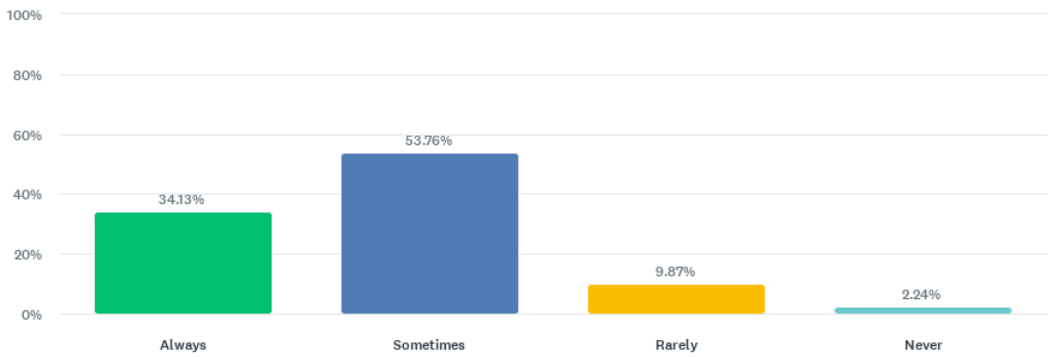
Perception of Social Media Information

A majority positioned themselves as 'neutral' (68.38%). Only 0.53% of the respondents have reported to 'fully trust' the information they see, whilst 15.28% reported to 'somewhat trust'. On the other hand, 12.97% have been reported to 'rarely trust' content from social media and 2.11% stated they 'do not trust at all'.

How much do you trust information you see on social media?

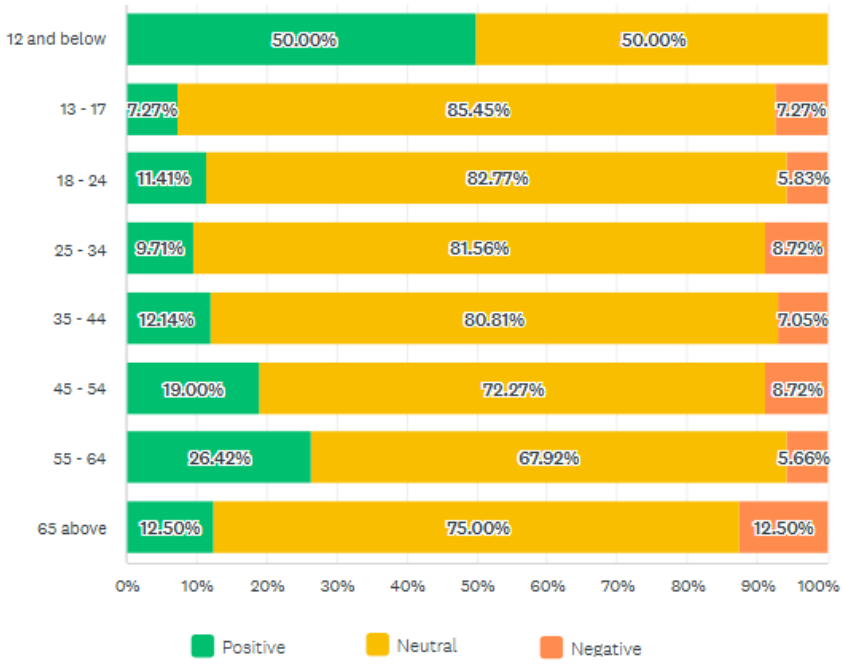


Have you ever come across misinformation, scams or extremist propaganda on social media?



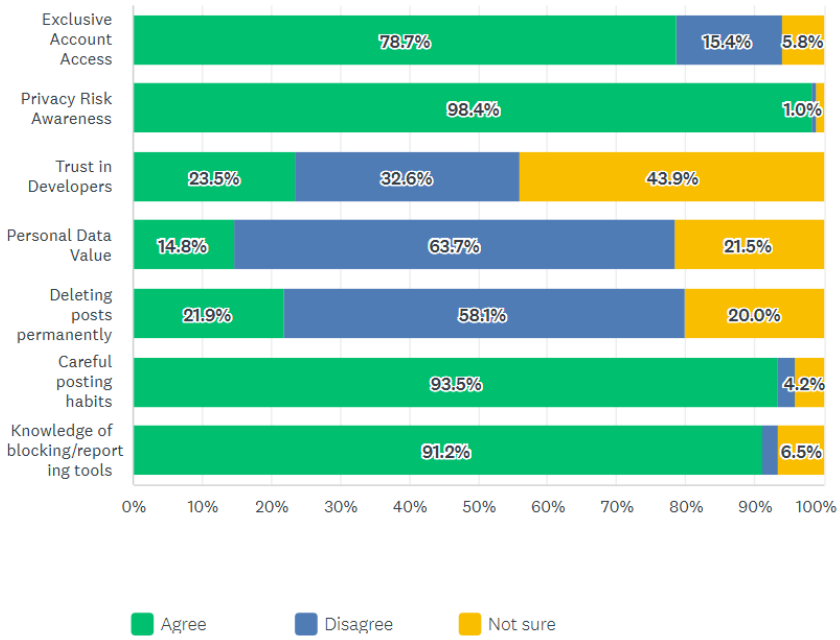
About half of the respondents stated that they come across the content mentioned only sometimes (53.76%), followed up by a concerning rate of always (34.13%) seeing such content. There are a small fraction of the respondents who rarely (9.87%) face this content and the least fraction had never (2.24%) come across such misleading content.

Do you think social media contributes positively or negatively to society?



Perceptions of social media are majoritively neutral across all ages ranging between 68% to 85%. The younger respondents aged 13 - 17 (85.5%) and 18 - 24 (82.8%) show the highest neutrality and with low negative views. Positive perception gradually increases with age, peaking at 26.42% at the age 55 - 64 years old.

Social Media Accessibility



- **Exclusive Access to Accounts**
  A majority of the respondents agree (78.7%) that they're the only person who has access to their social media accounts, while a small percentage have admitted otherwise (15.5%).

- **Awareness of Privacy Risks**
  98.3% of the total respondents showed a high level of awareness of privacy risk awareness.

- **Trust in Platform Developers**
  A small percentage of the total respondents believed that social media developers have done enough to keep their data safe (23.4%) while a larger total disagrees (32.6%). Meanwhile, a majority of the respondents were still unsure (43.9%).

- **Perceived Value of Personal Information**
  A majority of the respondents believe their data and personal information has value (63.7%), whereas a small yet concerning percentage believes that hackers have no interests with their personal information (14.7%).

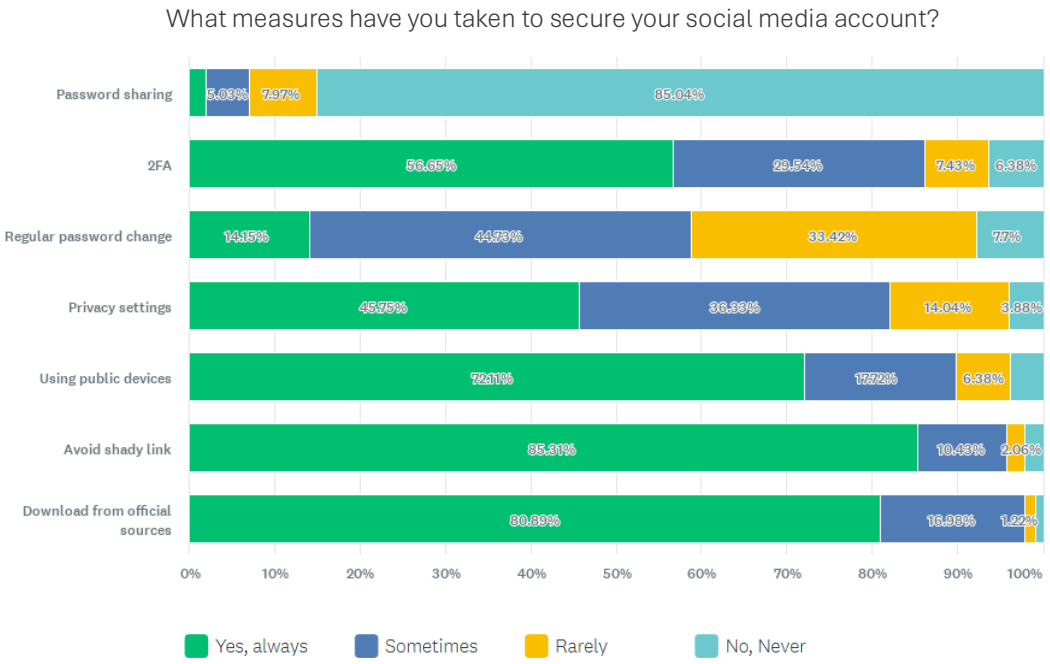
  For comparison, in 2022 (Cyber Safety Survey 2022, Page 3), 86% of the past respondents understood the value of their personal information and are aware of keeping that data from hackers.

- **Deleting Online Posts Permanently**
  58.1% disagreed indicating that a majority of respondents understand the term "permanent" of online content. Comparatively in 2022 (Cyber Safety Survey 2022, Page 3), results showed that 21% of the past respondents believed online postings can be deleted permanently.

- **Careful Posting Habits**
  The majority of the respondents reported that they carefully check before posting (93.4%), suggesting strong self-awareness in their online safety habits. Only 2.3% have answered to not checking their content before posting online.

- **Knowledge of Blocking/Reporting Tools**
  The vast majority of the total respondents have agreed to know how to block and report inappropriate content or accounts (91.2%), whereas a small fraction still disagreed (2.2%).

Social Media Account Security Habits



- **Sharing Social Media Passwords**
  A majority have reported that they never (85.04%) share their social media account passwords with friends or family, showing strong awareness of social media safety.

- **Enabling 2FA**
  More than half of the respondents have reported to always (56.65%) enable the 2FA feature, and some reported to do it sometimes (29.54%).

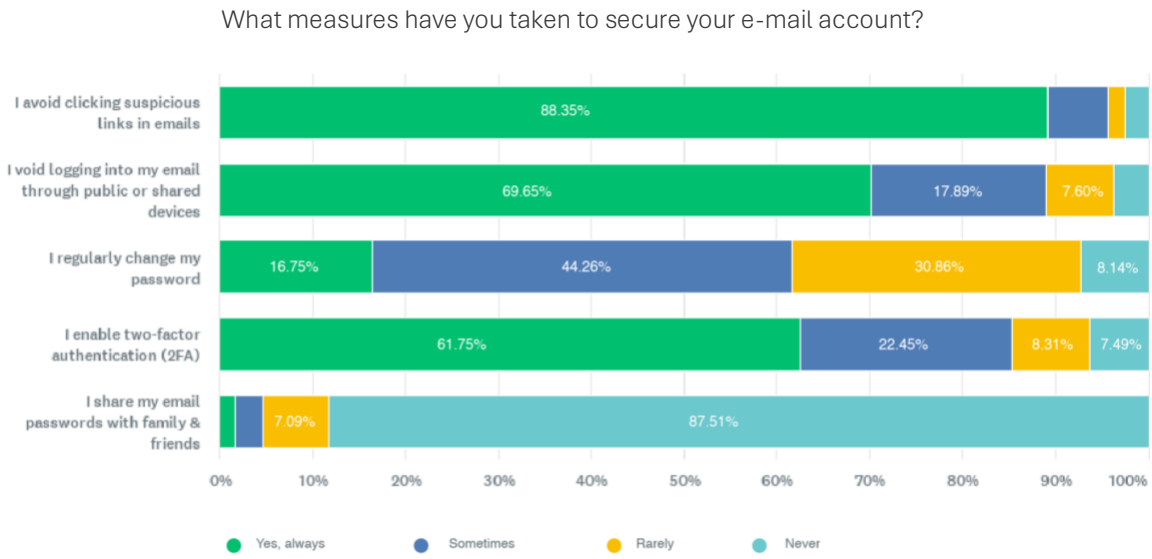
- **Regularly Changing Passwords**
  Only 14.15% of respondents have answered that they always change their passwords, while the majority were split between ‘sometimes’ (44.73%) and ‘rarely’ (33.42%).

- **Checking Application Privacy Settings**
  Almost half of the total respondents always (45.75%) check their application privacy settings, while some answered sometimes (36.33%) while a small percentage said they never (3.88%) check.

- **Avoiding Public or Shared Devices**
  A majority have reported they always (72.11%) avoid logging into their accounts through public or shared devices, whilst a few never (3.78%) avoid it.

- **Downloading Apps from Official Sources**
  A vast majority of the respondents have reported they always (80.89%) download their application from official app stores (Apple App Store, Google Play Store), while a few still admitted they never (0.91%) download from verified resources.

E-mail Account Security Habits



- **Sharing Email Passwords**
  The majority of the respondents have answered to never share their email passwords with friends nor family (87.51%), however there were still a small fraction admitted that they still share their passwords (1.96%).

- **Enabling 2FA**
  More than half have reported that they always enable 2FA for their email accounts (61.75%), and sometimes (22.45%). A small but concerning fraction admitted to never enabling 2FA (7.49%).

- **Regularly Changing Password**
  Only a few respondents have reported they always change their email passwords (16.75%),

and almost half of the responses have answered they sometimes (44.26%) change. A few respondents however answered that they have never changed at all (8.14%).

- Avoiding Public or Shared Devices
  The majority have reported to always avoid logging into their email through public or shared devices (70%), whilst a small group admitted they never avoid (4.86%) this habit.

- Avoiding Suspicious Links in Emails
  A high percentage has positively answered that they always avoid clicking suspicious email links (88.35%), although a minority admitted otherwise (3.21%).

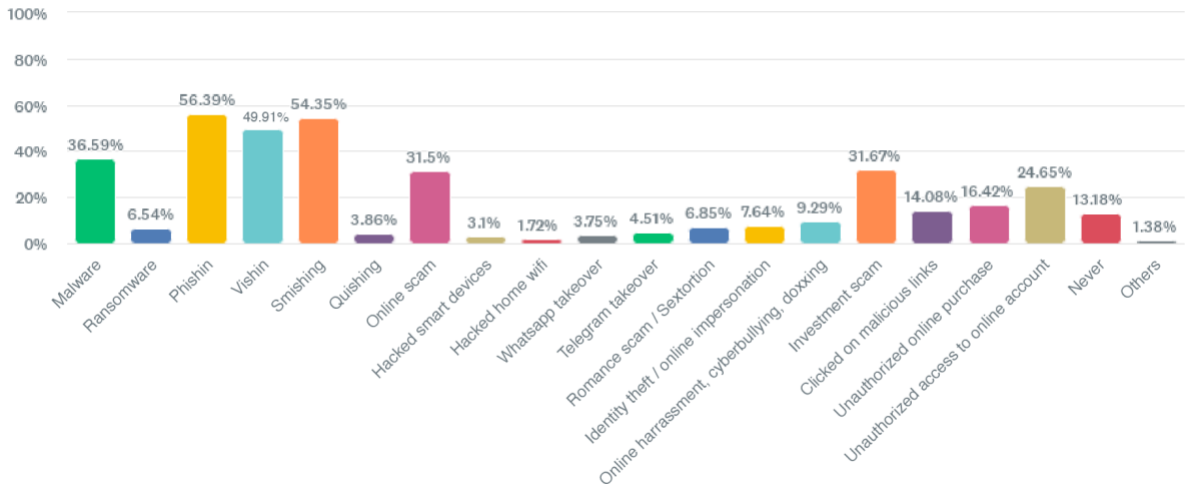
Comparison

In 2022 (Cyber Safety Survey 2022, Page 8), the top security measure was enabling two-factor authentication (67%), followed by avoiding sharing email password (54%), and changing password regularly (35%).

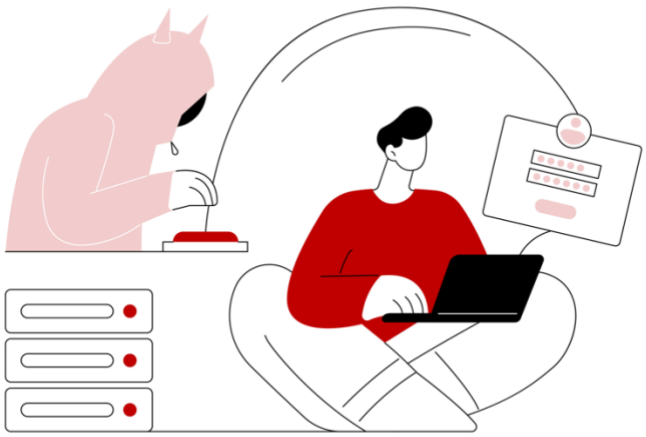
By the year 2025, new parameters were introduced, where 88% reported to avoid suspicious links, 87% avoided sharing email passwords and 70% avoided using public or shared devices.

SECTION 5

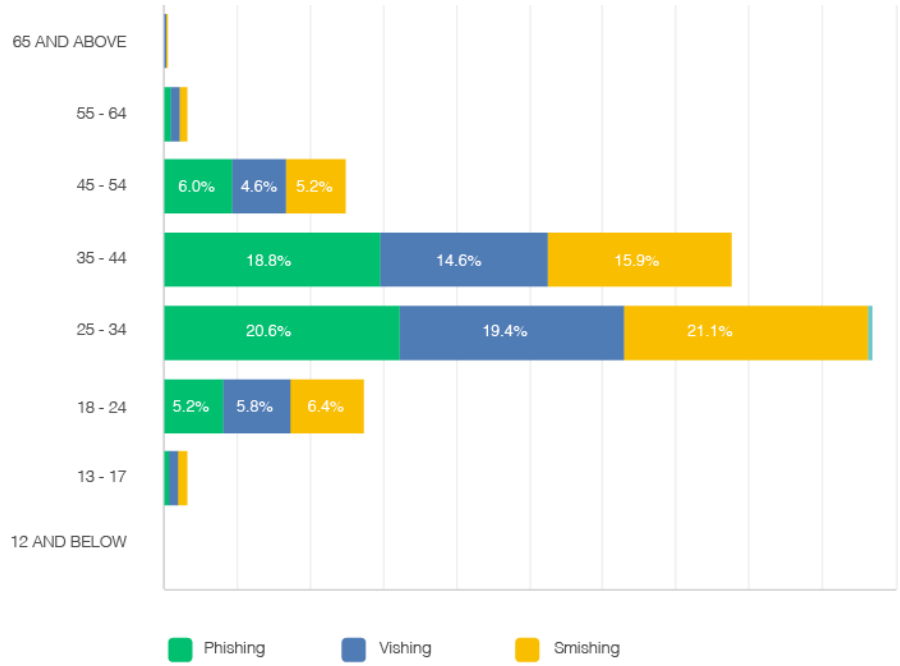
Personal Experiences



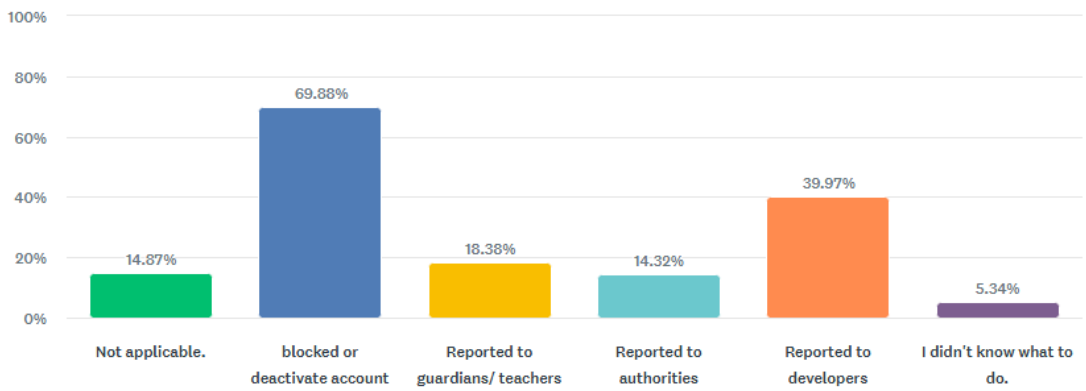
Three of the most reported incidents are phishing (56.39%), smishing (54.35%) and vishing (49.91%), remaining with the most pressing threats faced by current users. Only 13.18% of respondents have reported that they never experienced any cyber incidents.



Top 3 Experiences Based On Age

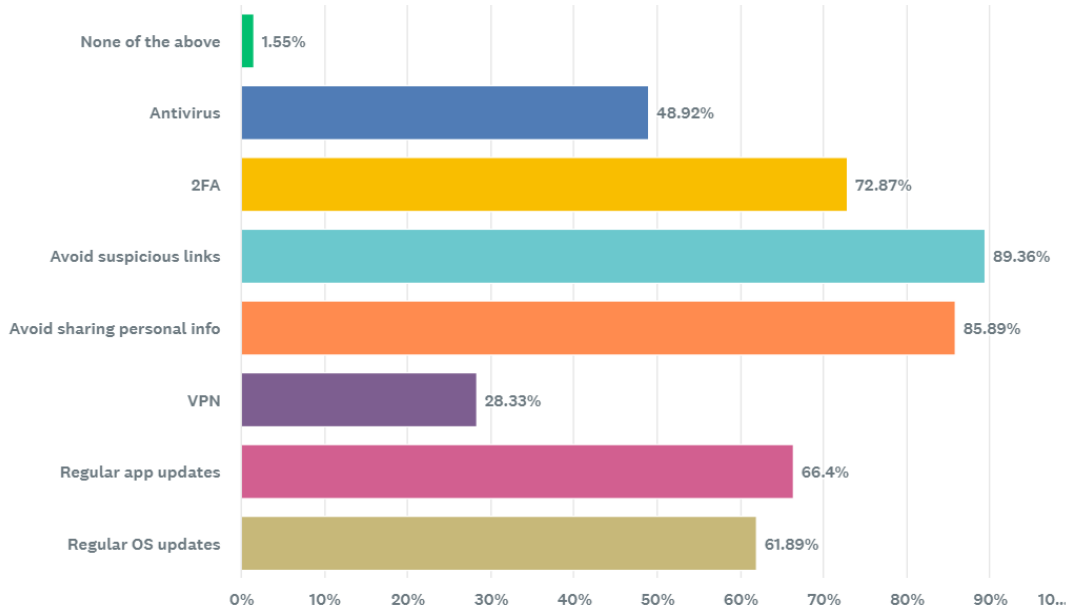


The chart above represents the age group of respondents to the top experience (Smishing, Phishing and Vishing). The age group 25-34 and 35 -44 years old has the highest exposure to phishing, vishing and smishing, specifically, smishing is the most reported in the age group 25-24 (21.1%), followed up by phishing (20.6%).



The highest choice of reaction recorded was blocking, deactivating or disabling their accounts or devices (69.8%), followed by reporting to organizations and developers (39.97%) such as banks and social media developers. 14.32% have answered that they reported to authorities like BruCERT or the law enforcement.

What are the precautionary steps that you've taken to prevent any cyber incidents?



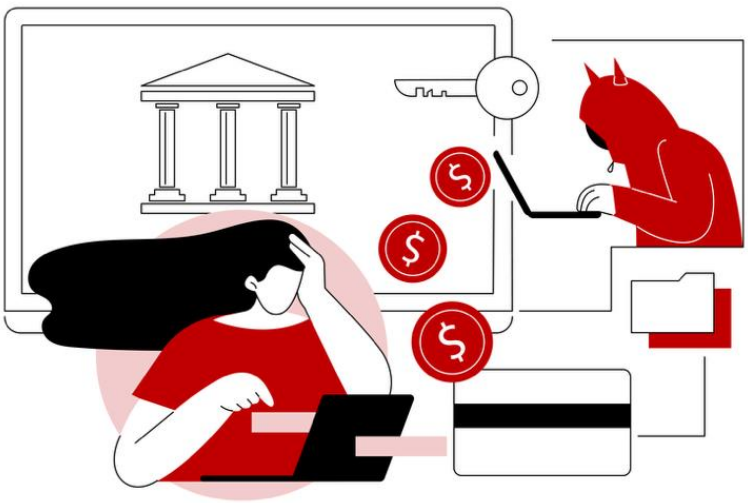
The two highest reports were avoiding suspicious links' (89.36%) and followed up by not sharing sensitive information online (85.89%). The other top answers were two-factor authentication (72.87%), keeping their devices updated (66.4%), and updating operating systems (61.89%).

Precautionary Measures Compared to 2022

By 2022 (Cyber Safety Survey 2022, Page 7) the majority reported avoiding suspicious links and avoiding sharing personal information, using 2FA and regular app updates. In 2025, the use of antivirus software dropped from 86% to 49%, while VPN use also fell from 55% to 28%.

SECTION 6

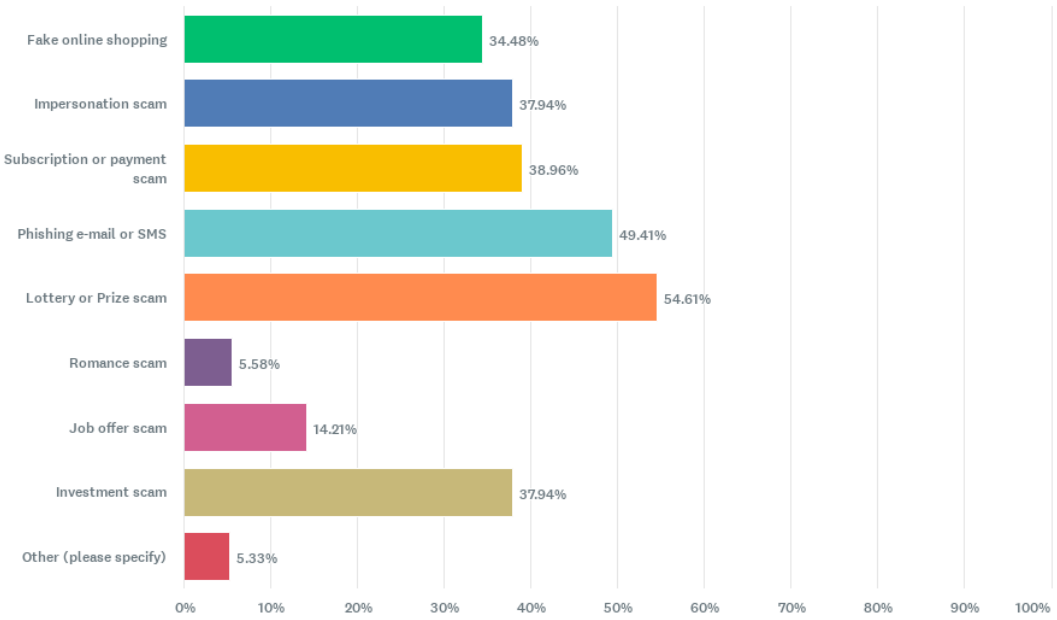
Online Scams



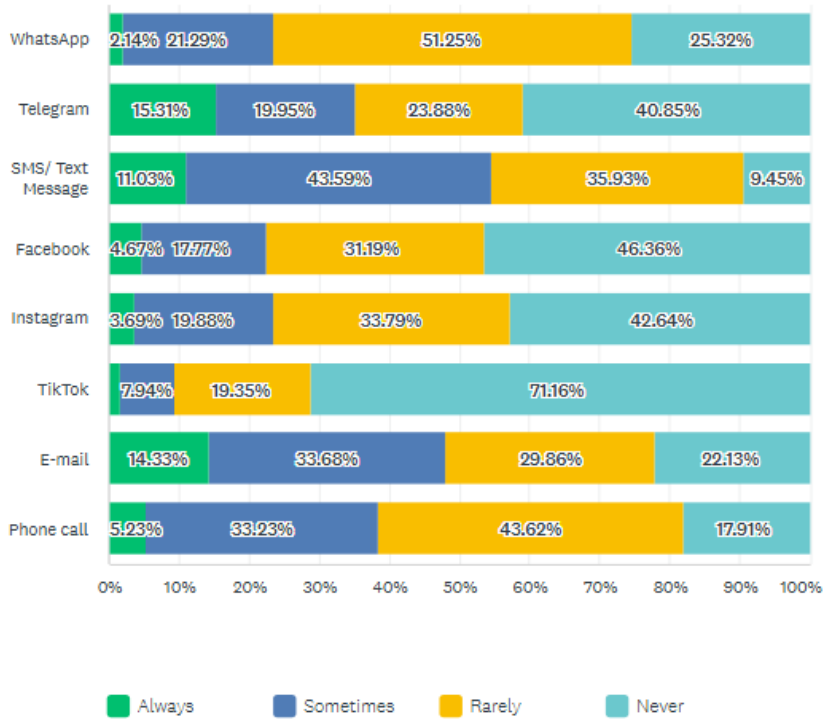
The survey has recorded a high level of respondents experiencing suspicious messages, emails or phone calls (80.12%), where majority of those experiences were Lottery or Prize scams (54.61%) and Phishing e-mail or SMS (49.41%).

Online Scam Frequency

If yes, what type?



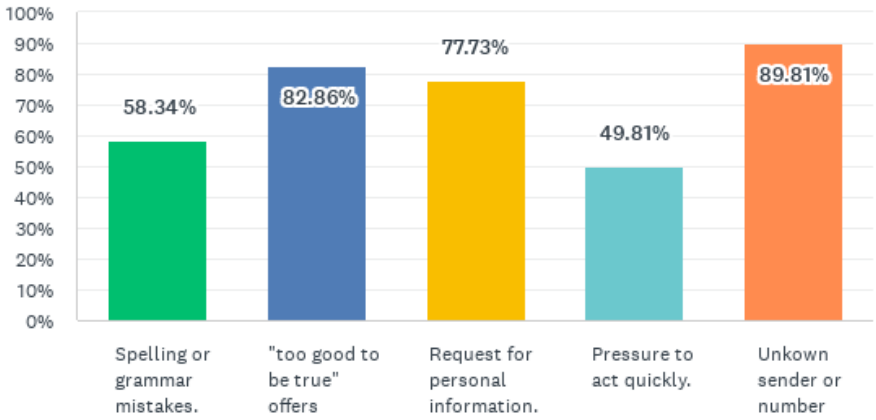
How often do you get scam messages from these platforms?



Telegram has the most risk of scam messages, with 15.31% saying they always receive scam messages. It is also most common through SMS or text messages and emails, where most of the respondents are always (54.6%) and sometimes (48.2%).

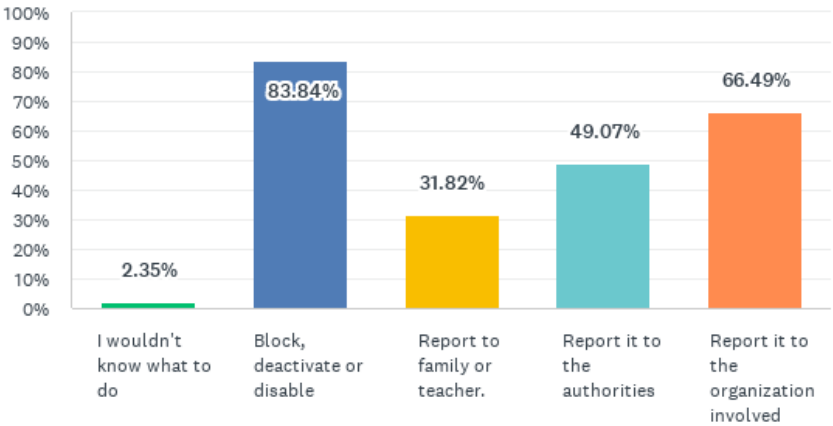
Identifying a Scam

What makes you suspicious of a scam?



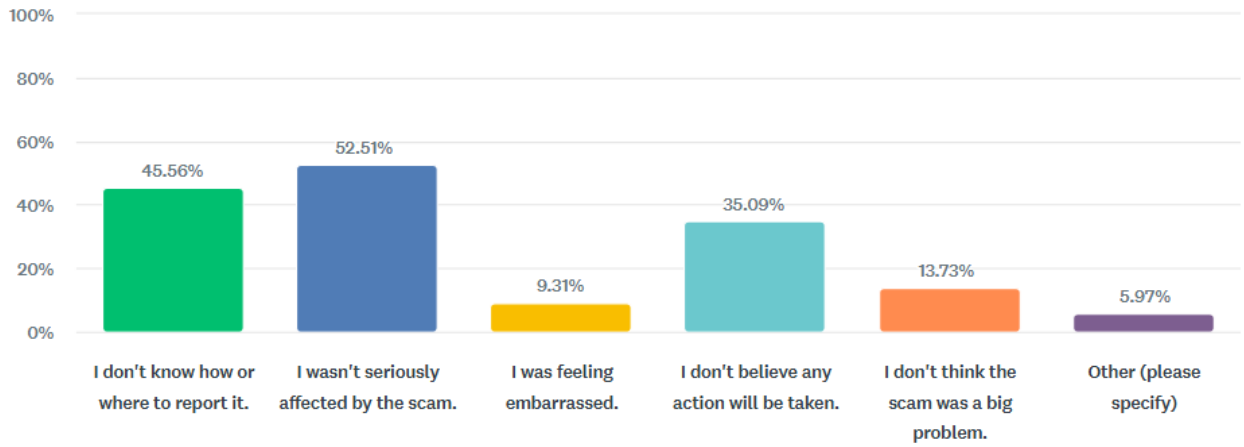
A total of 89.81% reported that “unknown sender or number” is the most obvious sign of a scam, followed closely by offers that seem “too good to be true” (82.86%) of respondents and requests for personal information (77.73%).

If you became the victim of an online scam, what would you do first?



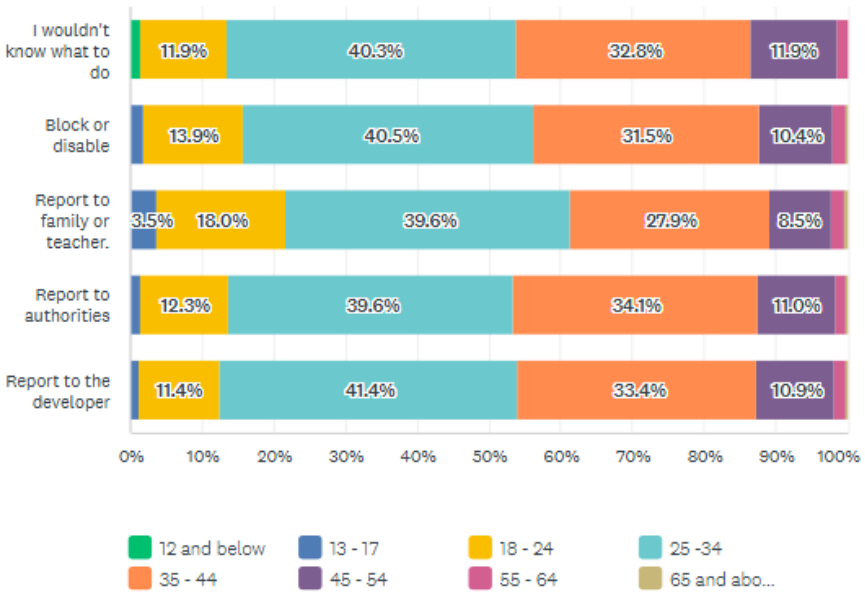
The majority of the respondents chose to block, deactivate or disable (83.84%) as their first reaction, followed up by reporting to the involved organizations (66.49%) such as banks or service providers. Nearly half of the total respondents have answered they would reach out to the authorities (49.07%).

What might stop you from reporting a scam?



The two most common reasons preventing them from reporting were not feeling seriously affected by the scam (52.51%) and felt unsure how or where to report it (45.56%). A number of respondents have also expressed doubt that any action will be taken (35.09%) when reporting, while a small percentage have admitted to feeling both experiencing no major effect by the scam (13.73%) and feeling embarrassed (9.31%).

Comparison by Age Group

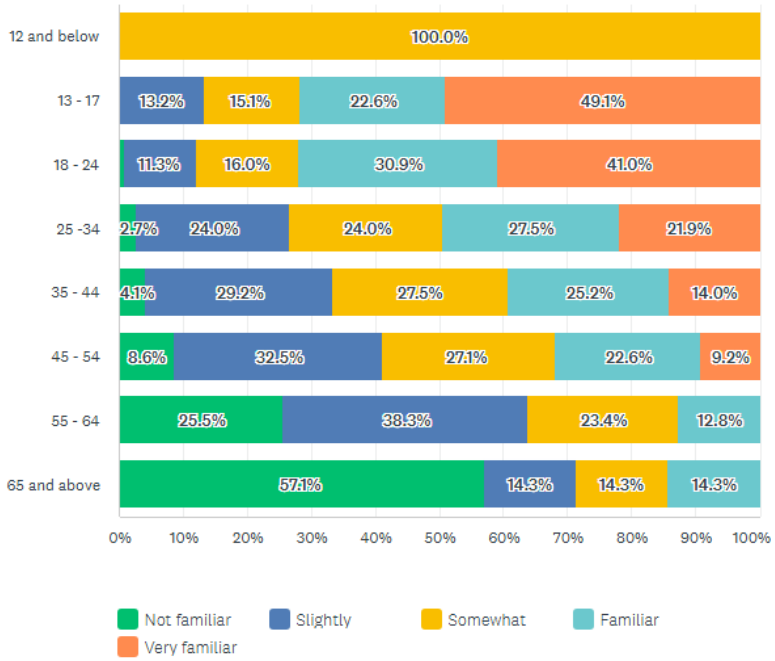


Grouping the respondents by age, all age groups have reported they would block, disable or even report the scam to the authorities or the developers involved as their first step. The age group between 25-34 years of age has the majority total in all responses options.

SECTION 7

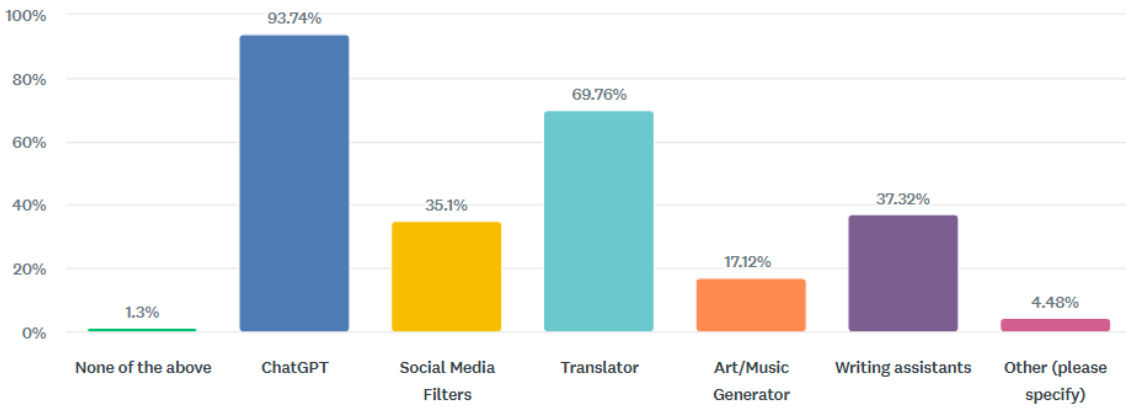
Artificial Intelligence (A.I.)

How familiar are you with Artificial Intelligence (A.I.) platforms?



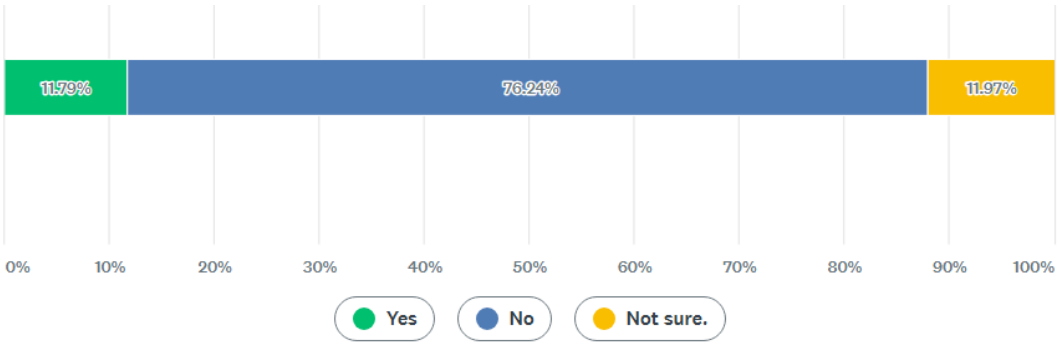
Respondents aged 13 - 17 years old had the highest familiarity with Artificial Intelligence, with 49.1% answered very familiar, while working-age adults show more consistent levels of familiarity across categories; from slightly familiar to very familiar.

What A.I tools or platforms have you used before?



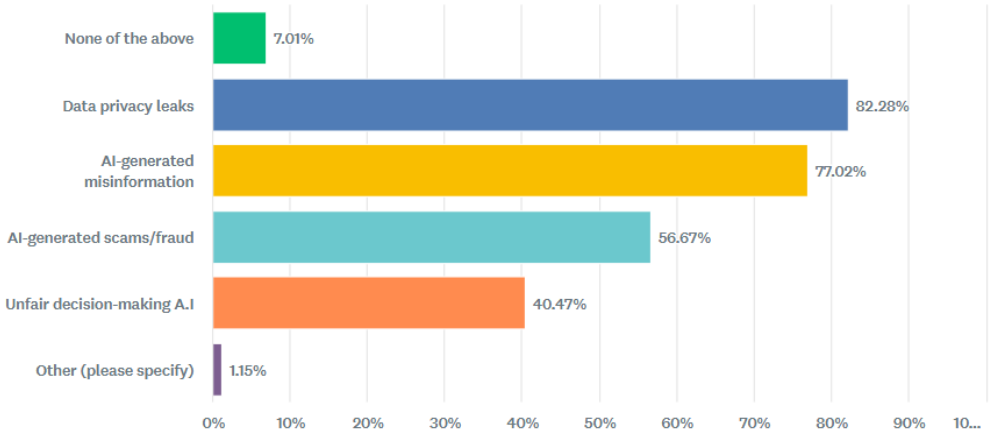
ChatGPT is the most widely used platform among the respondents, with 93.74% recorded. Other popular tools include translators (69.76%) and writing assistants (37.32).

Have you ever shared yours or anyone's personal information with an A.I platform?



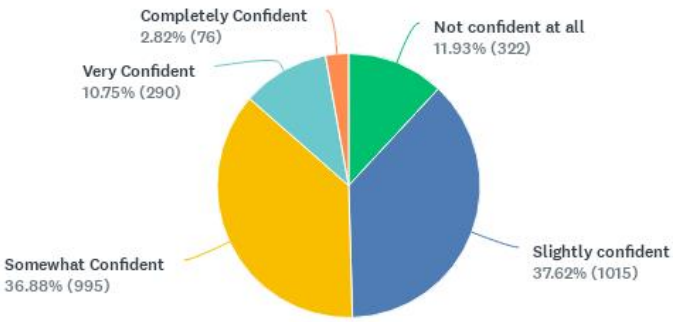
A majority have reported that they do not share personal information (76.24%) with an AI platform. A small percentage have admitted that they do share (11.79%).

Are you aware of any of these A.I-related risks?



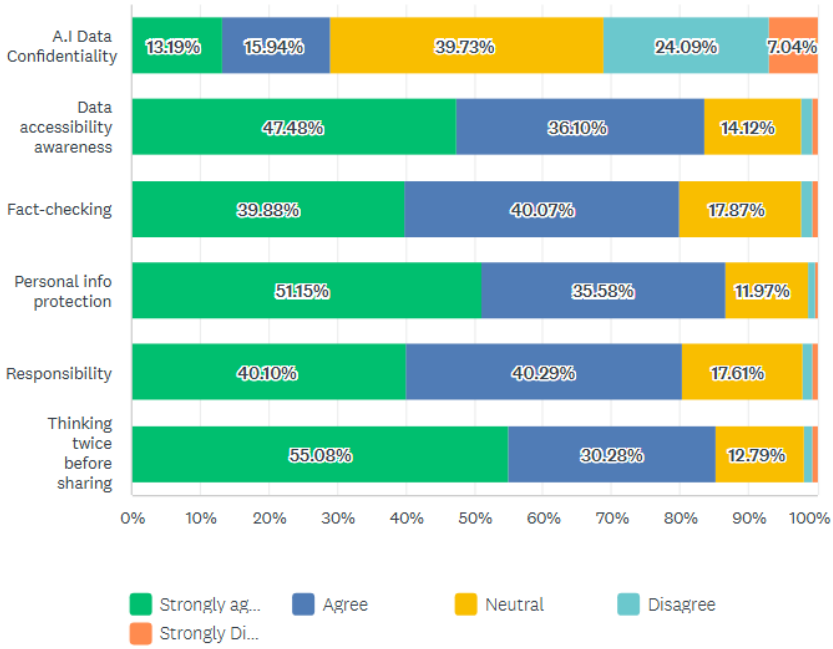
The top two majority are aware of data privacy leaks caused by oversharing with A.I platforms (82.28%) and awareness of A.I-generated misinformation (77.02%).

How confident are you in identifying A.I-generated content?



The majority of the respondents have admitted to be slightly confident (37.62%) and somewhat confident (36.88%).

Rate how much you agree to all these following statements.



- I always think twice before sharing personal information

  A majority of the respondents showed a strong caution, where they have responded strongly agree (55.08%) and agree (30.28%) to always rethink before sharing personal information.

- I am aware that A.I platforms store, use or share the data I provide

  Most respondents have answered to strongly agree (47.48%) and agree (36.10%) with being aware of how A.I platforms control the data provided.

- I am aware of protecting any personal or sensitive information

  Higher respondents percentage answering strongly agree (51.15%) and agree (35.58%) have indicated high precautious trait towards their cyber safety

- I am confident that A.I platforms keep the data I share confidential

  Only small percentages have strongly agreed (13.19%) and agreed (15.19%) with how AI platforms keep the data confidential.

- I am well prepared to use A.I platforms responsibly and safely

  The high positive response have indicated the responsible engagement with AI tools, with respondents answering strongly agree (40.10%) and Agree (40.1%)

- I double check anything an A.I tells me

  A fraction of the respondents will always verify A.I results indicating user's resilience on fact-checking and verifying, evidently the response showing strongly agree (39.88%) and agree (40.07%).

SECTION 8

Conclusion

The overall findings suggest that there is growth in cybersecurity awareness among respondents, reflected in their ability to identify suspicious messages, understand common scam attempts and practice precautionary measures when going online. Fortunately, a majority of the respondents shows cautious behaviour towards common signs of cyber threats such as unknown senders, 'too good to be true' offers and requests for personal information. This also indicates that exposure to awareness messages have a positive impact. However, there is a concern about the drop in usage of security tools. The latest survey indicates the use of antivirus software dropped from 86% to 49% , while VPN use also fell by half from 55%.

Digital accessibility and social media continue to play a major role in bringing awareness about online safety experience. With a vast majority of the respondents are actively connected through multiple accounts and platforms, the risk of encountering scams like phishing, misinformation or even impersonation remains significant. Many users do show cautious behaviour and distrust towards unknown sources. However, exposure to fake messages persists, especially through emails, text messages and chat applications like WhatsApp and Telegrams are still concerningly high.

Therefore, awareness of online threats has become more widespread. However, there is still room for improvements, where awareness messages still need to be delivered consistently and confidence grows in the population to identify and react.