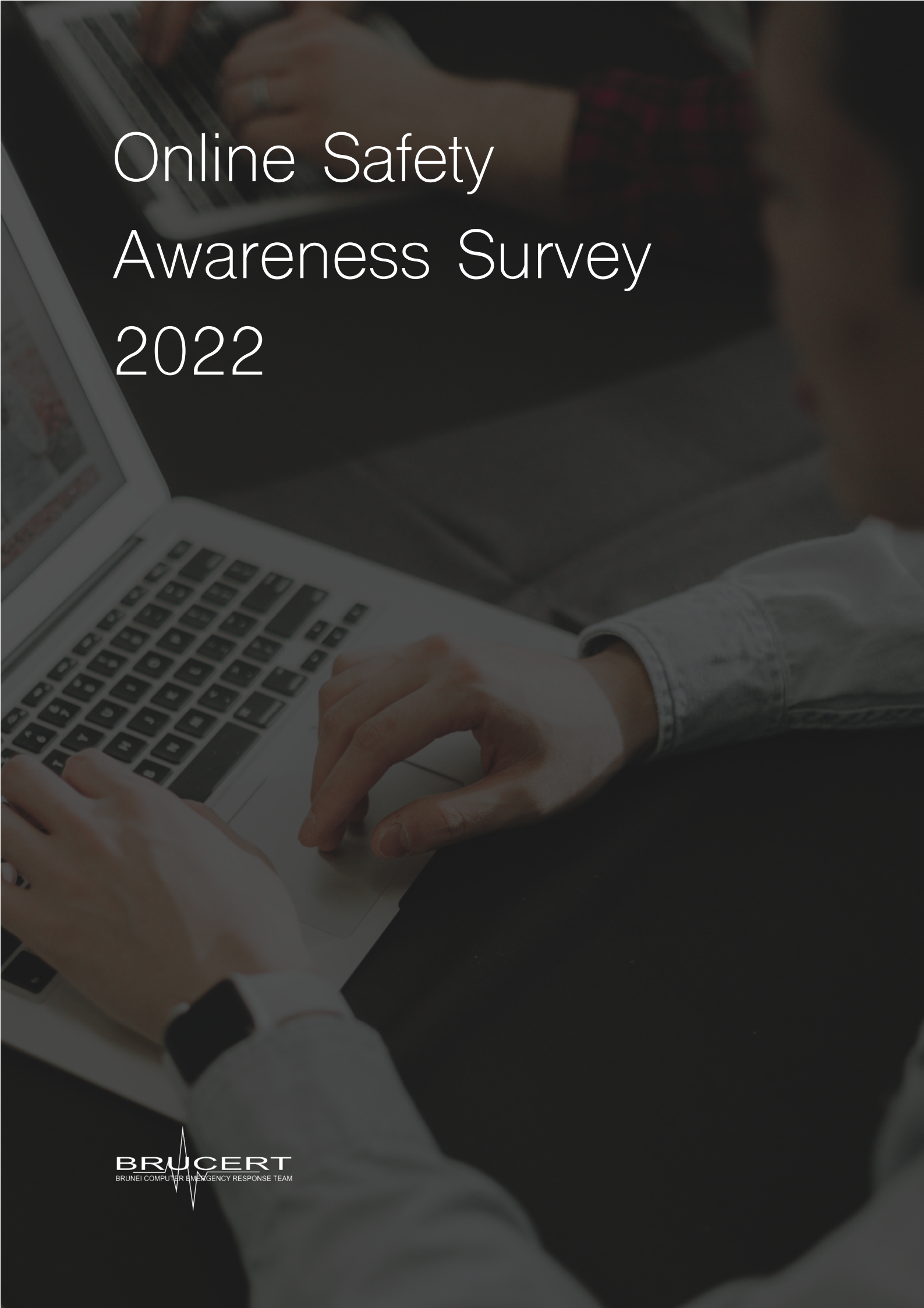
Online Safety Awareness Survey 2022



BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

Table of Contents

Introduction 2

Methodology 2

Demographics 2

Attitude Towards Cybersecurity 3

Value of personal information 3

Think before you post 3

Cybersecurity is everyone's concern 4

Ability to recognize scams 4

Cybersecurity Incidents 5

Precautionary measures 7

Securing Accounts 8

Securing personal email accounts 8

Securing social media accounts 8

Sharing passwords 9

Two-Factor Authentication (2FA) 9

App safety 11

Installing apps 11

Removing apps 11

Public wi-fi 12

Reporting Cybersecurity Incidents 13

Misdirected reporting 13

Likelihood of reporting 13

Introduction

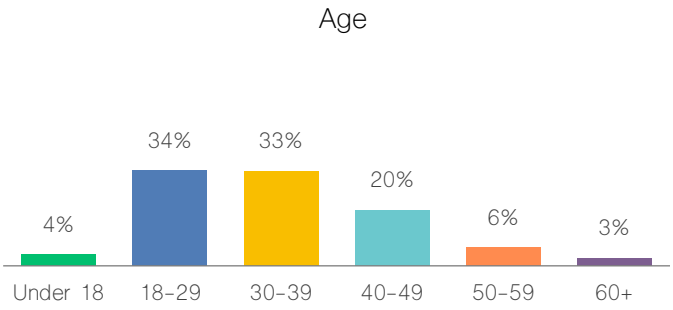
Brunei Computer Emergency Response Team (BruCERT) under Cyber Security Brunei (CSB) conducted an online survey from 7th to 21st June 2022 to study the attitude and behaviour of the general public towards online safety.

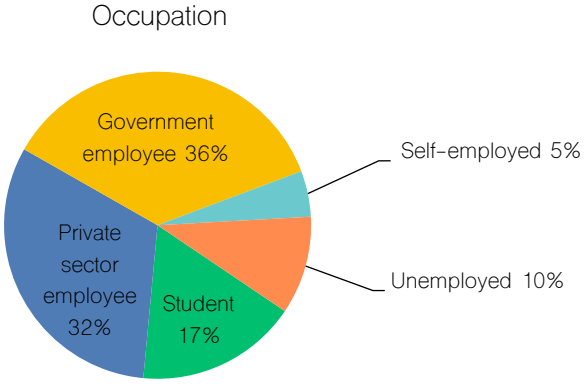
Methodology

This survey was conducted through an online survey form which was publicized to the public via the official *Gov.bn* Telegram account, BruCERT and Cyber Security Brunei's social media accounts, and at the BruCERT exhibition booth during Brunei Mid-Year Conference and Exhibition 2022 (MYCE) at the International Convention Centre.

Survey participation was voluntary with the offer of lucky draw prizes, with 3 winners selected at random from the pool of responses. The survey was open for a period of 2 weeks and the final sample size was 1,326 responses.

Demographics

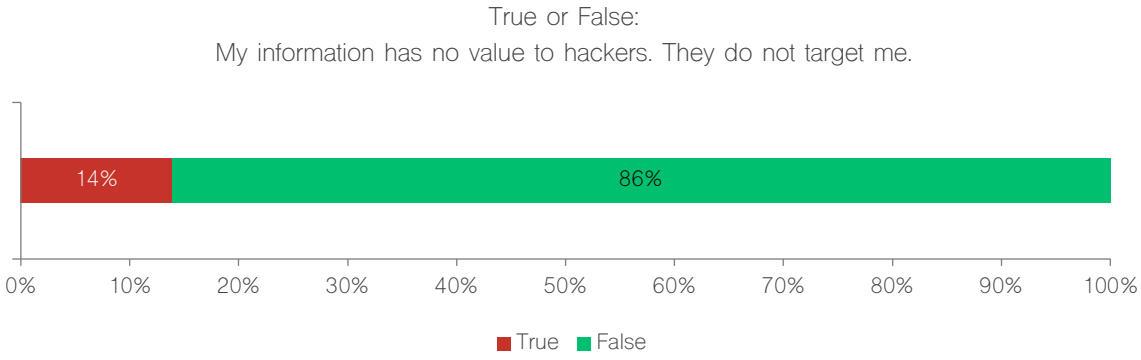




Attitude Towards Cybersecurity

Value of personal information

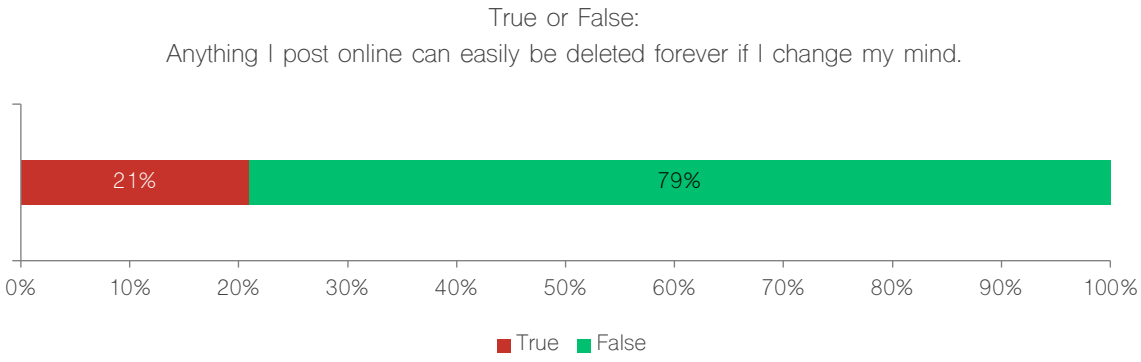
14% of respondents believe that their information has no value to cyber criminals and that they would not be targeted by hackers.



The age group who agreed with this statement the most were children. 35% of those under the age of 18 believe that they will not be targeted by hackers.

Think before you post

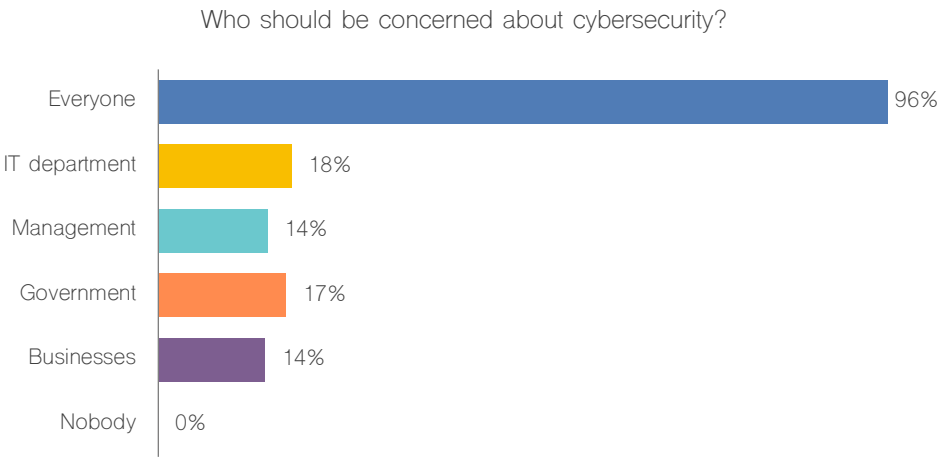
21% of respondents believe that their online posts can easily be removed if they change their mind about it.



Children are especially prone to this attitude – 49% of respondents under 18 years old agreed with the statement.

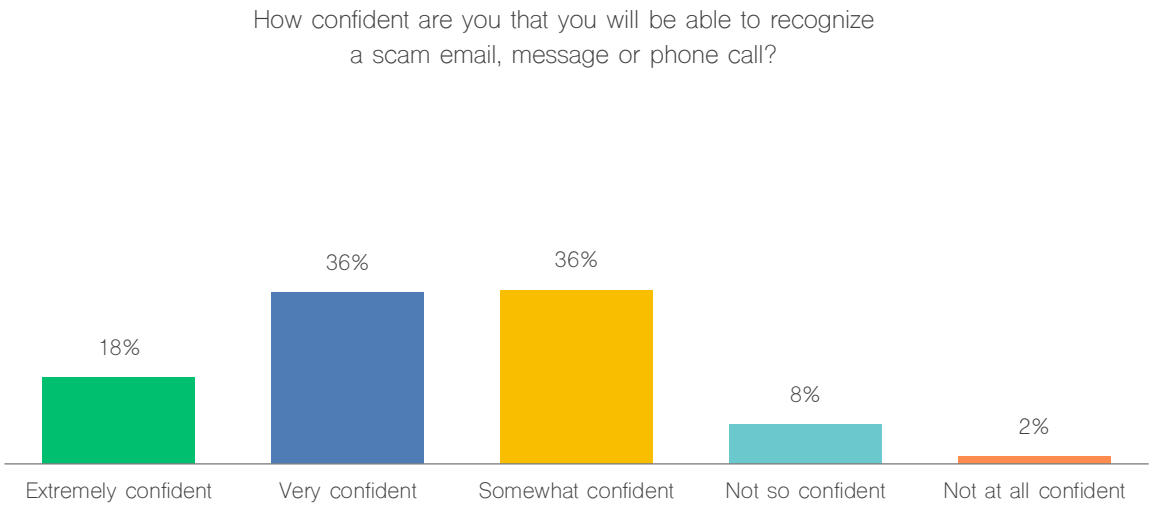
Cybersecurity is everyone's concern

96% of respondents agree that everyone should be concerned about cybersecurity.



Ability to recognize scams

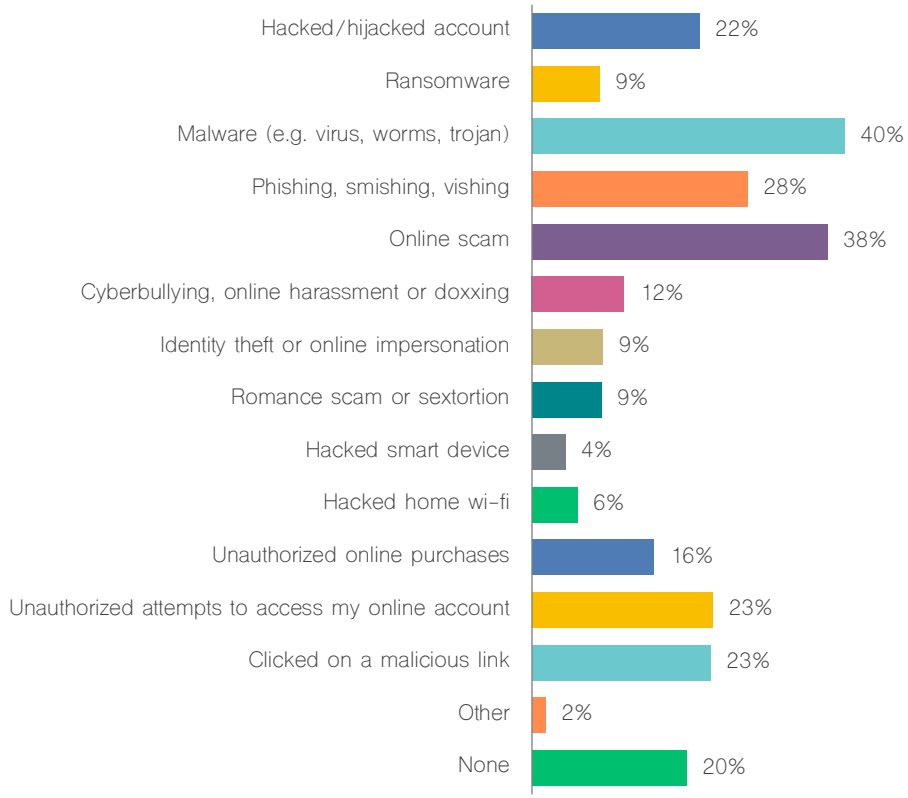
Most people are confident that they can recognize a scam email, message or phone call when presented with one.



Cybersecurity Incidents

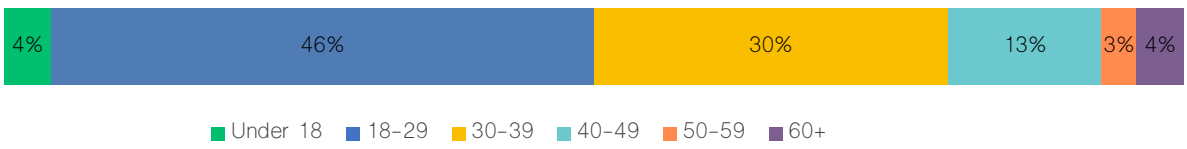
The three most common types of cyber incidents experienced in the past year are **malware**, **online scams**, and various forms of **phishing**. 20% of respondents did not encounter any cyber incidents.

In the past year, what kind of cyber incidents have you personally experienced?



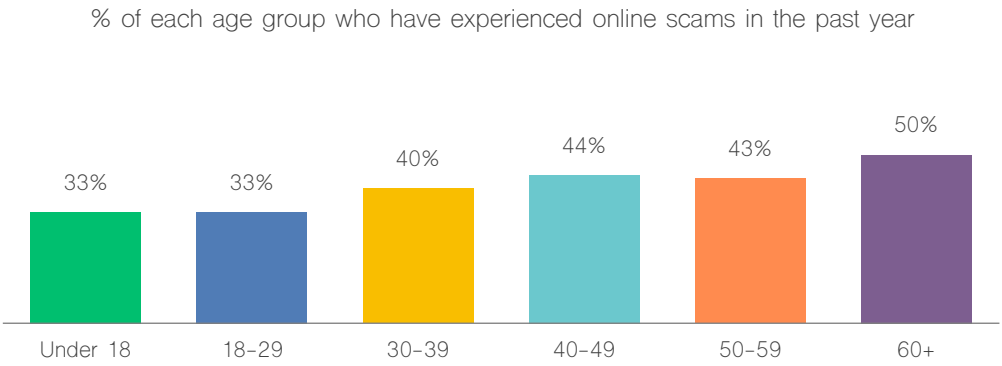
Cyberbullying, online harassment or doxing

50% of those who had experienced cyberbullying, online harassment or doxing in the past year comprise of people aged below 30.



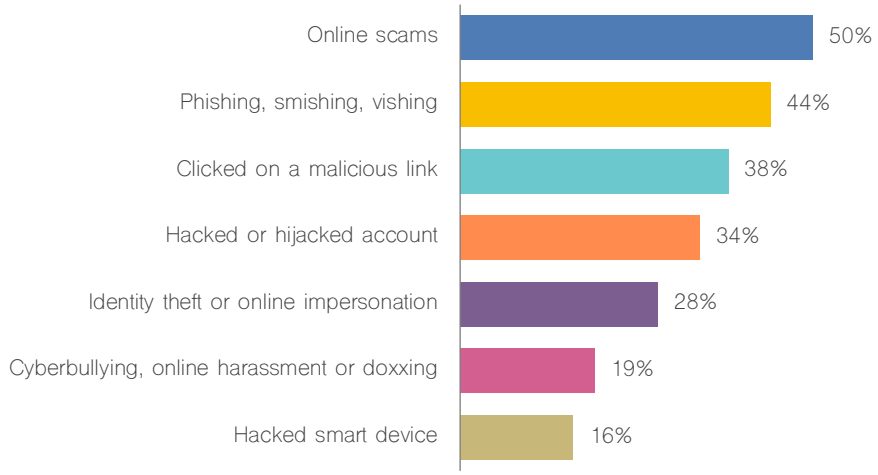
Online scams

Online scams appear to be affecting older individuals. In the past year, online scams have affected only one-third of people aged below 30, but half of those aged over 60.



Incidents affecting senior citizens

Respondents aged 60 and above are the most prevalent age group to encounter certain types of cybersecurity incidents. The numbers below indicate the percentage of senior citizens who have experienced these incidents in the past year.

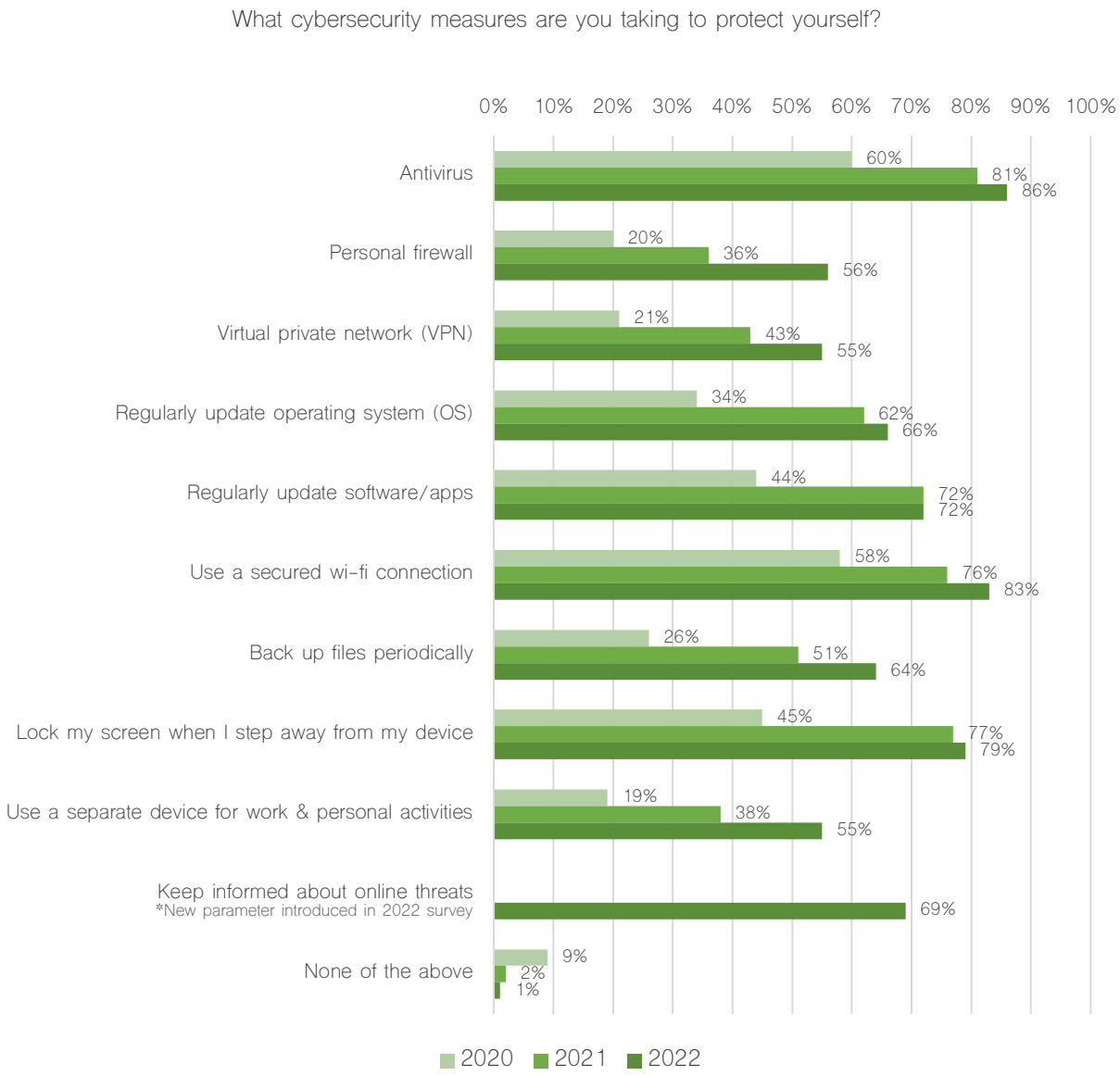


Precautionary measures

Respondents were asked what cybersecurity measures they are taking to protect themselves. The top 3 precautions taken are **antivirus** software, using a **secured wi-fi** connection, and using a **screen lock** on devices.

Comparison to previous years indicates a **positive trend with increased adoption of cybersecurity measures** across the board. Most notably, there has been significant increase in the use of personal firewall, virtual private network (VPN), and using separate devices for work and personal activities.

69% of respondents try to stay informed about the latest online threats. Only 1% admitted to not taking any protective measures.

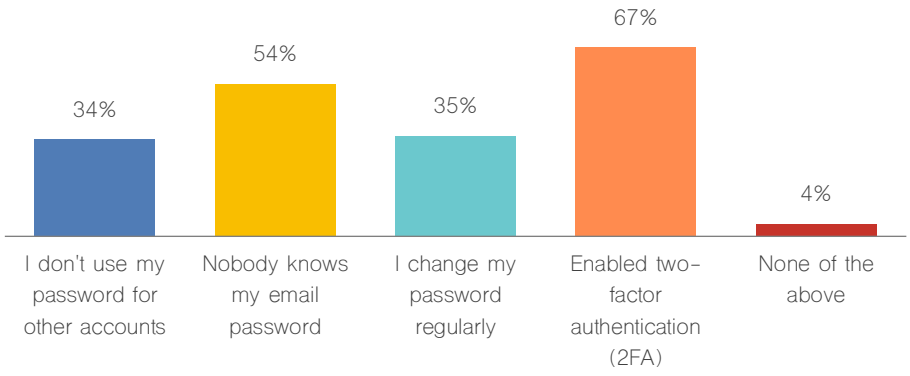


Securing Accounts

Securing personal email accounts

Two-thirds (67%) of respondents have enabled two-factor authentication (2FA) to secure their personal email accounts, and one-third (34%) use a unique password which is not reused for other accounts. Only 4% have not made any effort to secure their personal email account.

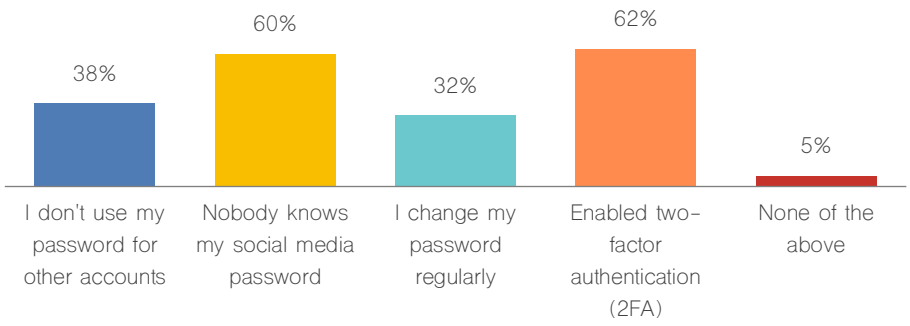
What measures have you taken to secure your personal email account?



Securing social media accounts

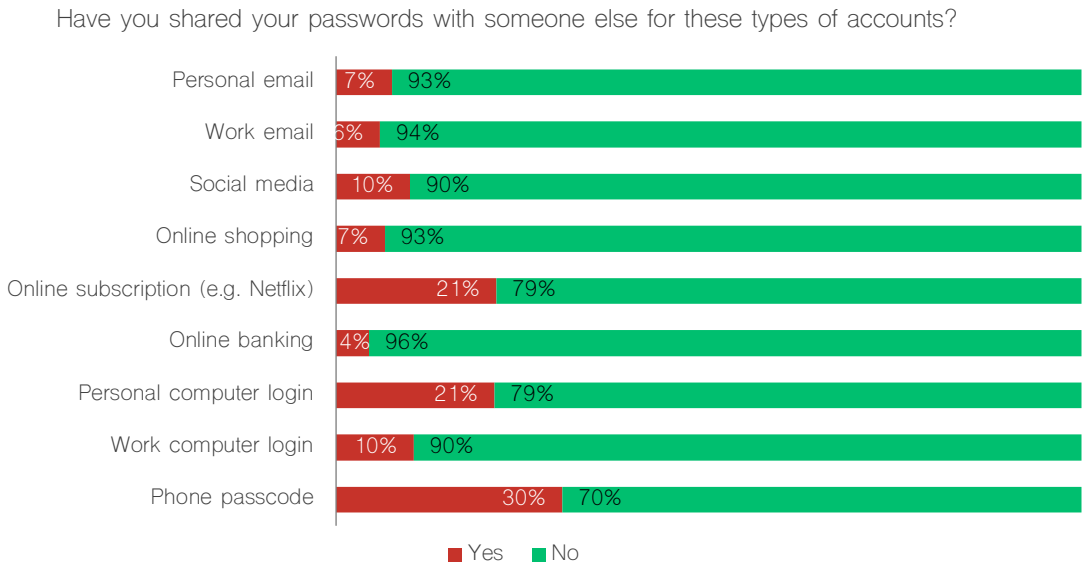
Similarly, 62% have enabled 2FA for their social media account, and only 5% have not made any effort to secure their social media account.

What measures have you taken to secure your social media account?



Sharing passwords

Respondents were asked if they share their passwords for various types of accounts and devices. The most shared password is the phone passcode, while the least shared is the password for online banking.



Passwords for personal devices

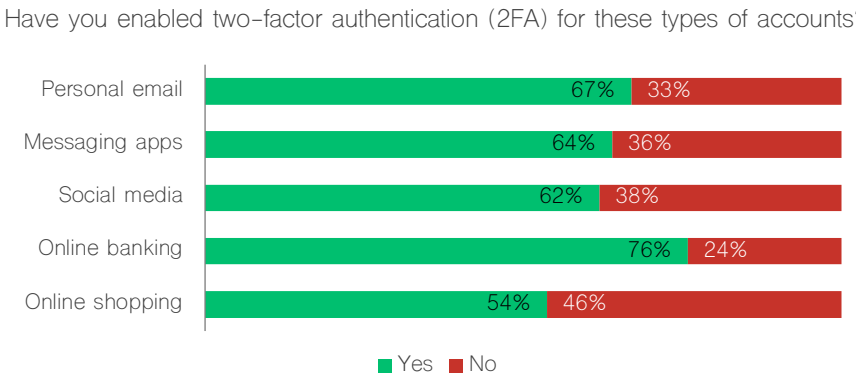
30% of respondents have shared their phone passcode, while 21% have shared their personal computer login.

Passwords for work

10% have shared the login password for their work computer, while 6% have shared the password for their work email account.

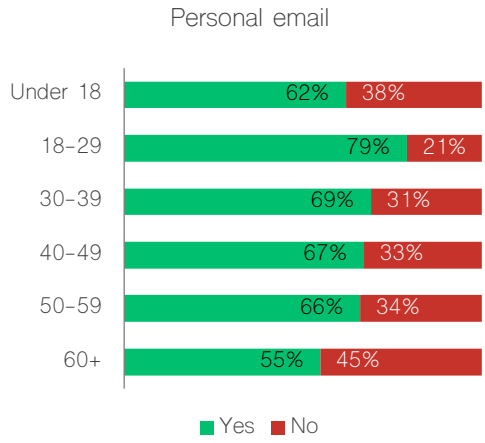
Two-Factor Authentication (2FA)

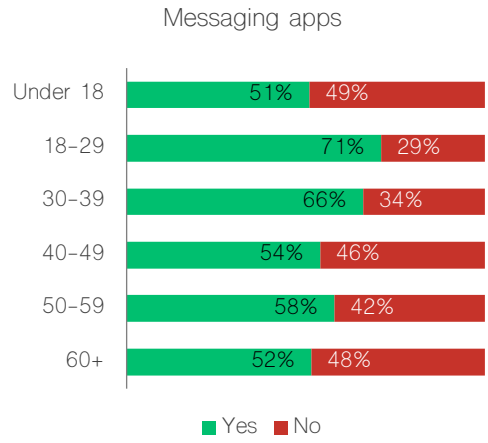
Two-factor authentication is most commonly enabled for online banking, with three-quarters of respondents utilizing it for that purpose.

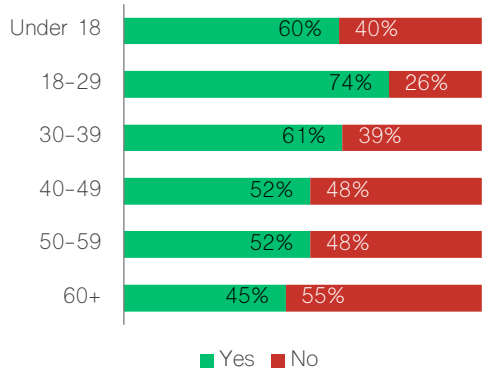


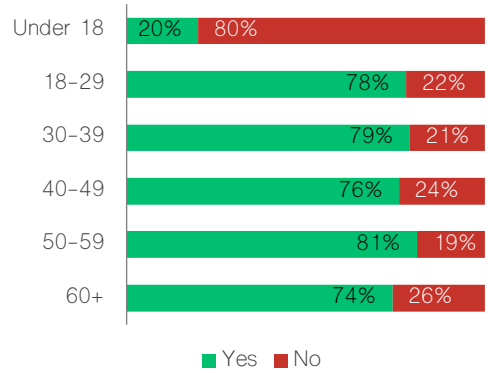
Comparison by age

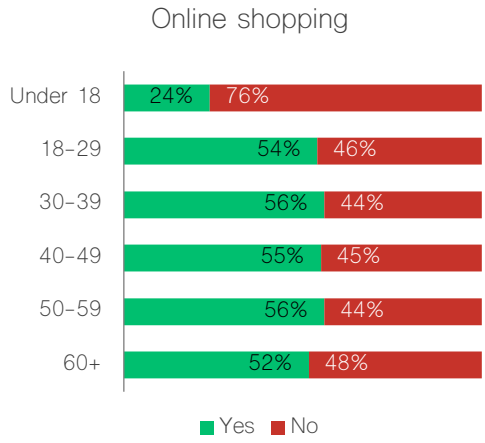
The 18-29 age group are the largest age group to enable 2FA for personal email, messaging apps and social media. This may be an indication that these services bear the most importance to this age group.







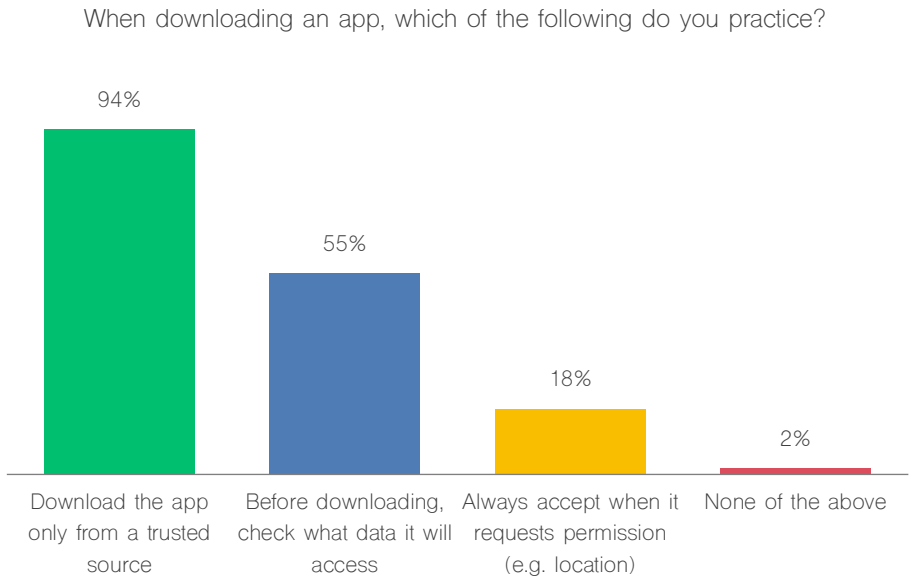




App safety

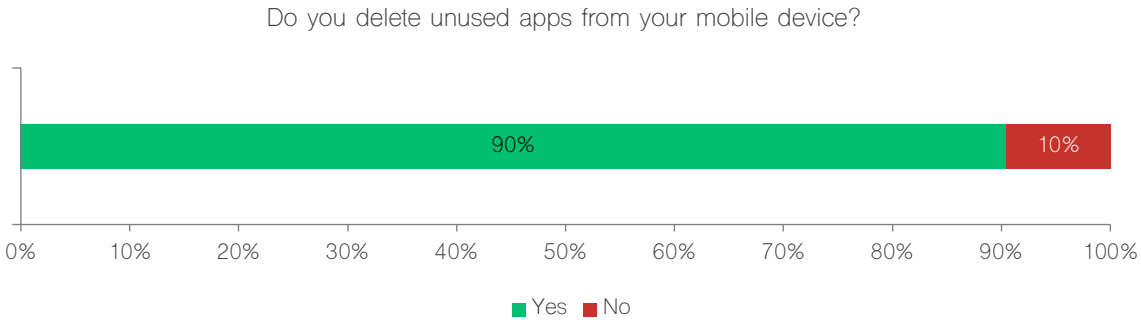
Installing apps

Respondents were asked what precautions they take when it comes to installing mobile apps. Over half of respondents said they first check what kind of data would be accessed by the app before downloading it. 94% said they only download apps from a trusted source.



Removing apps

Outdated apps and software can make a device vulnerable, so it is important to remove unused apps to reduce the risk. 90% of respondents delete unused apps from their mobile device.

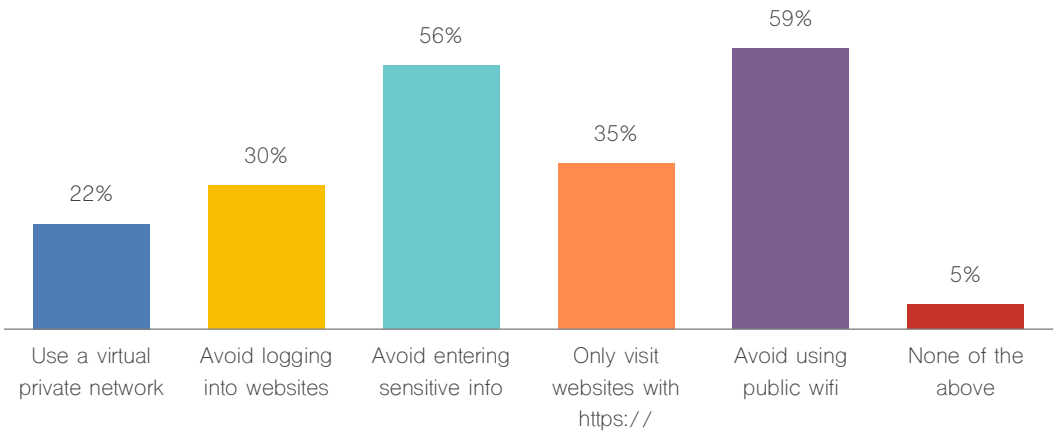


Public wi-fi

More than half (56%) of respondents said they avoid entering sensitive information when connected to a public wi-fi network. About one-third would only visit encrypted websites, and one-third avoid logging into websites while on public wi-fi.

Only 22% use a virtual private network (VPN) to encrypt traffic when connected to public wi-fi networks. 59% of respondents play it safe and avoid using public wi-fi altogether.

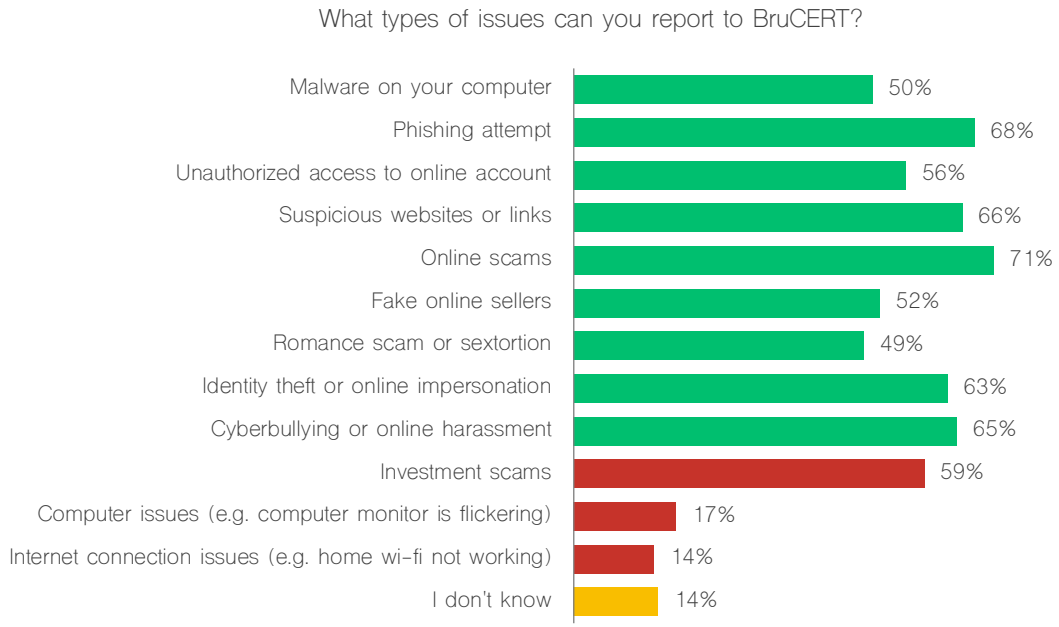
When using public wi-fi, what precautions do you take?



Reporting Cybersecurity Incidents

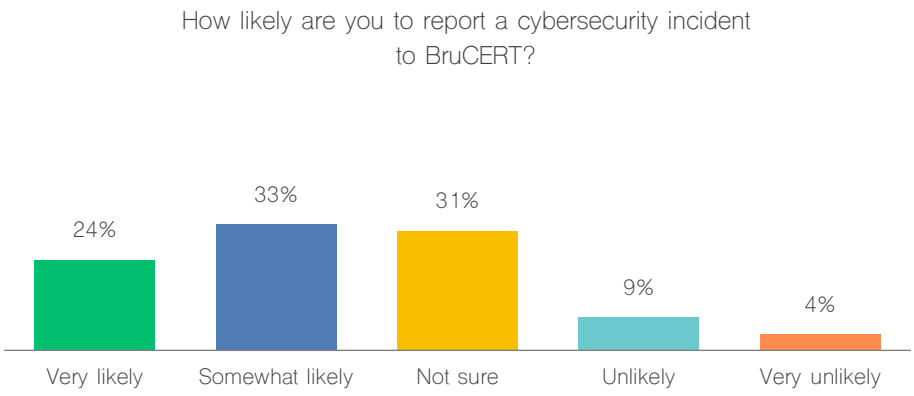
Misdirected reporting

59% of respondents have a misconception that investment scams should be reported to BruCERT, and some believe they should contact BruCERT about technical problems with their computer or internet connectivity issues. 14% of respondents are not aware of what should be reported.



Likelihood of reporting

Over half (57%) of respondents said they would report cybersecurity incidents to BruCERT, while 31% are unsure and 13% are not likely to report.



About BruCERT

Brunei Computer Emergency Response Team (BruCERT) is the national referral agency dealing with computer-related and internet-related security incidents in Brunei Darussalam. It is one of the core services offered by the national cyber security agency Cyber Security Brunei (CSB) under the Ministry of Transport and Infocommunications (MTIC). BruCERT is the central hub which coordinates with international CERTs, network service providers, government agencies, and other relevant organizations to facilitate the detection, analysis, and prevention of security incidents on the internet.

Secure Verify Connect is BruCERT's public awareness campaign created to raise awareness of online safety and information security among the Bruneian public. Please visit www.secureverifyconnect.info or www.brucert.org.bn for more information.

CSB
CYBER SECURITY BRUNEI

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

SVC secure verify connect