GSMA Intelligence

Towards an inclusive digital nation: building trust in the digital age in Asia Pacific

February 2024

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Follow the GSMA on X: @GSMA

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Author

Kenechi Okeleke, Senior Director, GSMA Intelligence

Contributor

Jeanette Whyte, Head of Public Policy, GSMA Asia Pacific

Contents

Executive summary

The digital world continues to grow rapidly as people and businesses increasingly use online platforms to interact and perform daily tasks. By the end of 2023, there were 4.7 billion mobile internet subscribers around the world, equivalent to nearly three out of five people in the world. Asia Pacific is home to more than 1.4 billion mobile internet subscribers, equivalent to just over half of the region's population; these figures will rise to 1.8 billion and 61%, respectively, by the end of this decade.

Mobile connectivity has had a transformational impact on people, businesses and wider society, enabling access to many life-enhancing digital services and driving productivity gains from the application of digital technologies to business processes. However, bad actors also operate in the digital world as much as they do in the physical, continuously expanding the scope and scale of online threats and finding new ways exploit vulnerabilities. Additionally, online threats are particularly difficult to tackle considering that the nature of digital technologies, which makes it possible for perpetuators to operate in anonymity and from any location.

The advent of AI tools, including generative AI (genAI) presents opportunities and risks for online safety. As a force for good, AI's capabilities make it an ideal tool for identifying and preventing online threats. However, the same technology in the hands of bad actors can be a tool to perpetuate online threats by making it harder to track cyberattacks. As such, the democratisation of advanced AI tools from the launch of several genAI platforms and the integration of AI applications into end-user devices could have a profound impact on the online threat landscape.

The evolving online threat landscape is capable of eroding confidence and trust in digital services. For instance, the World Economic Forum has identified misinformation and disinformation as the foremost global risk in the short term, especially in the context of major elections in 2024 in several populous countries that together account for nearly half of the global population, including Bangladesh, India, Indonesia and Pakistan. Consequently, the need to address this and other prevalent threats has never been more urgent.

The benefits of participating in the digital world for people and businesses are not in doubt. This is the premise for the increasing focus on digital nationhood by governments in Asia Pacific and beyond. Governments, mobile operators and social media platforms all have a role to play here. Across Asia Pacific, these stakeholders have introduced various measures to improve online safety and build trust, some more than others. But for everyone it is a race against time, considering the ever-increasing and evolving scope of online threats.

Importantly, the task of maintaining and enhancing trust must be viewed as a shared responsibility between stakeholders, as opposed to the sole responsibility of any single stakeholder. This highlights the need for open dialogue and cooperation between all parties in the digital ecosystem. This white paper highlights five steps to support existing measures by the various stakeholders and inspire new ones:

- **Awareness**: Stakeholders should take steps to create more awareness around online threats and solutions to help people and businesses stay safe online.
- **Education**: People and businesses need to be equipped with 'digital resilience' skills (knowledge of how to navigate and respond to risks) to help them become confident digital citizens.
- **Collaboration**: Collaboration within and across industries is essential to facilitate information sharing, resource pooling and efforts to take a common approach in tackling various threats. This may also involve cooperation with law enforcement in cases where the threat is illegal.
- **AI opportunity**: In the emerging AI era, it is important for stakeholders to take advantage of the opportunity that AI presents to mitigate existing online threats and counter new ones.
- **International cooperation**: Online threats often transcend geographical boundaries and local jurisdictions. Regional and global cooperation is required to prevent such threats to improve online safety and build trust.

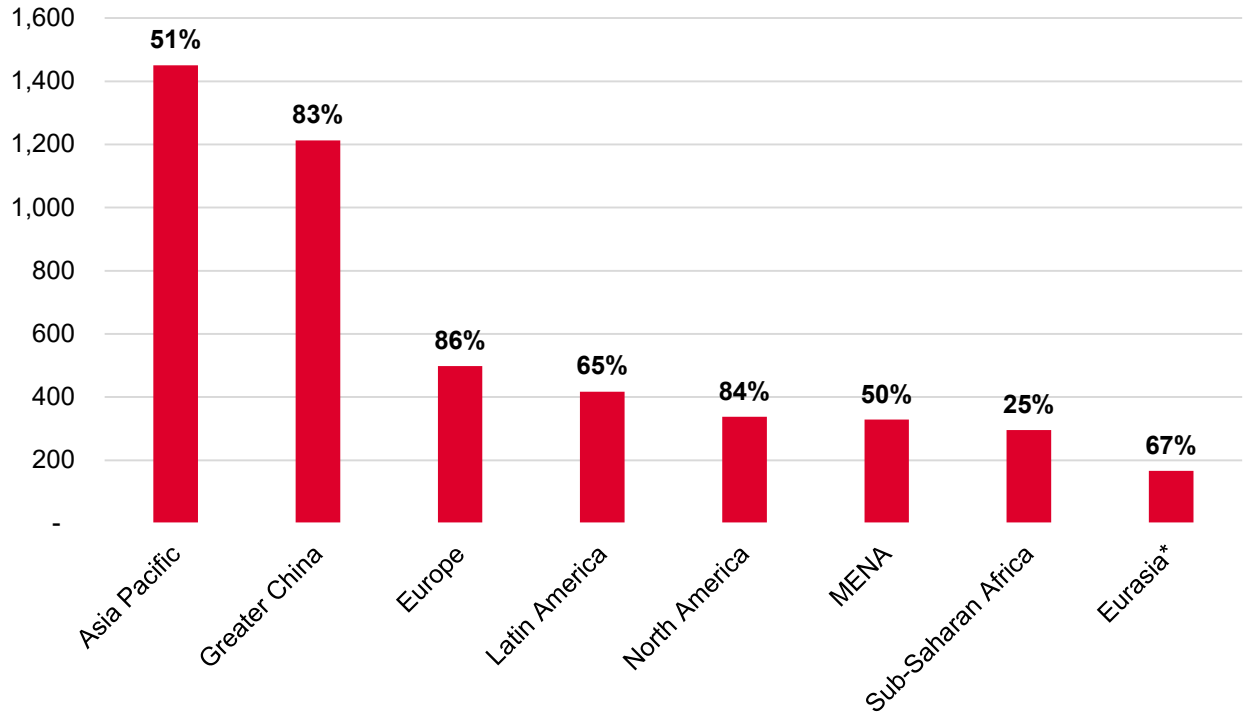
As part of its ongoing stakeholder dialogue on online safety and trust in digital services in Asia Pacific, the GSMA welcomes comments on this white paper. To submit feedback, please contact the GSMA at apac_enquiries@gsma.com.

1. The online threat landscape

The digital world continues to grow rapidly as people and businesses increasingly use online platforms to interact and perform daily tasks. At the end of 2023, there were 4.7 billion mobile internet subscribers around the world, equivalent to nearly three out of five people in the global population. Asia Pacific is home to more than 1.4 billion mobile internet subscribers, equivalent to just over half of the region's population. Usage of many online services, such as shopping and entertainment, is at an all-time highs and still growing, while remote working and access to healthcare, education and other essential services have become the norm in many instances.

Figure 1: Number of mobile internet subscribers and penetration by region, 2023
Million, percentage of population

Source: GSMA Intelligence



* Includes Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan

Mobile connectivity has had a transformational impact on people, businesses and wider society, from allowing businesses to increase productivity and better utilise scarce resources to helping governments improve citizens' welfare and protect the environment. Indeed, future digital nations will thrive on the integration of digital technologies in every aspect of the economy and, importantly, the ability of citizens to access and use digital services within a safe online environment.

1.1 The scope of online threats in Asia Pacific

Bad actors operate in the digital world as much as they do in the physical, continuously expanding the scope and scale of online threats and finding new ways exploit vulnerabilities. Online threats are particularly difficult to tackle considering the nature of digital technologies, which makes it possible for perpetuators to operate in anonymity and from any location. Moreover, assessing the impact on victims can be more challenging, as online threats can have a profound psychological impact beyond other quantifiable impacts, such as financial losses. This can take a mental toll on victims, resulting in loss of trust in digital platforms, which can in turn alienate individuals and communities from beneficial online services.

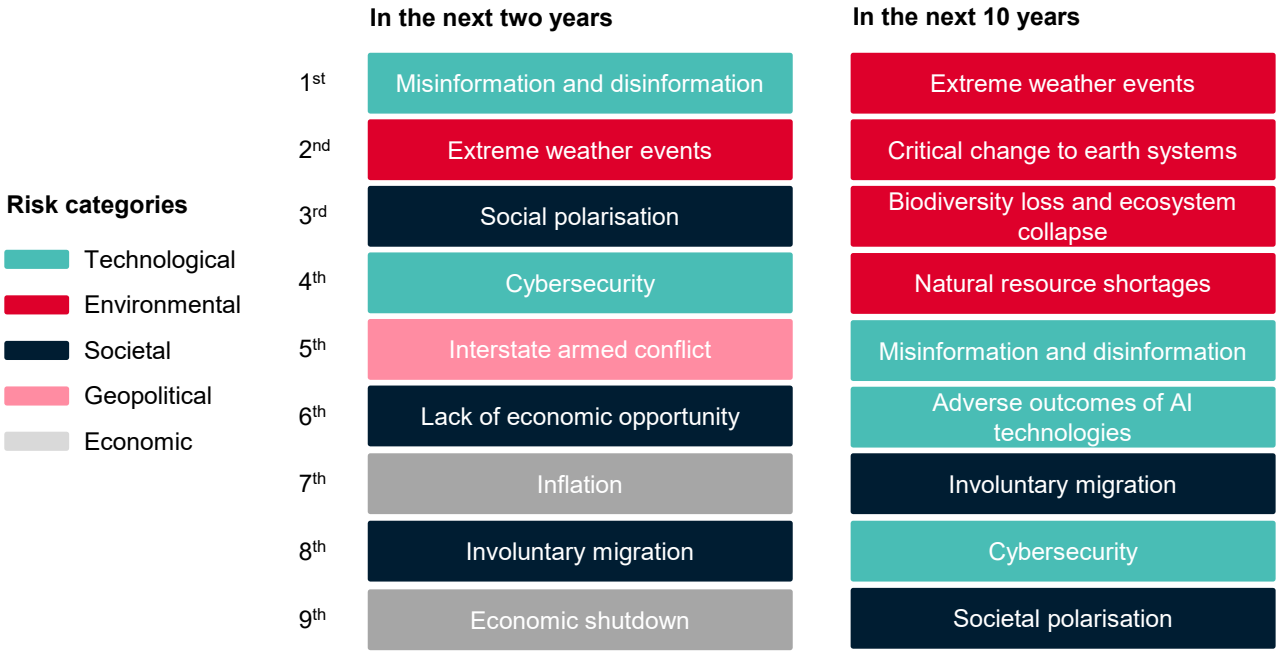
The types of online threats vary considerably in scope and scale: some threats target vulnerable individuals and groups, such as the elderly and children; some are intentionally malicious, while others are inadvertent (albeit with similar negative effects on victims); and some threats appear to be more widespread, while others are more prevalent in certain communities due to the socioeconomic and cultural factors at play.

Enterprises are also susceptible to various online threats, including data breaches, which can result in considerable financial and reputational losses, and distributed denial of service (DDoS) attacks, which can lead to severe disruptions and operational downtime. Most enterprises consider the internet as an indispensable business tool. However, concerns around security, reliability and quality of service, and the potential for these to result in major business disruption, can threaten confidence and trust.

Online misinformation and disinformation are an example of an online threat with a global footprint. The World Economic Forum has identified these as the foremost global threat in the next two years (cybersecurity ranked fourth), especially in the context of major elections in several populous countries, including Bangladesh, India, Indonesia and Pakistan in Asia Pacific, as well as the UK and the US, during that period (see Figure 2).[1]

Figure 2: Global risks ranked by severity over the short and long terms
Please estimate the likely impact (severity) of the following risks over a two-year and 10-year period

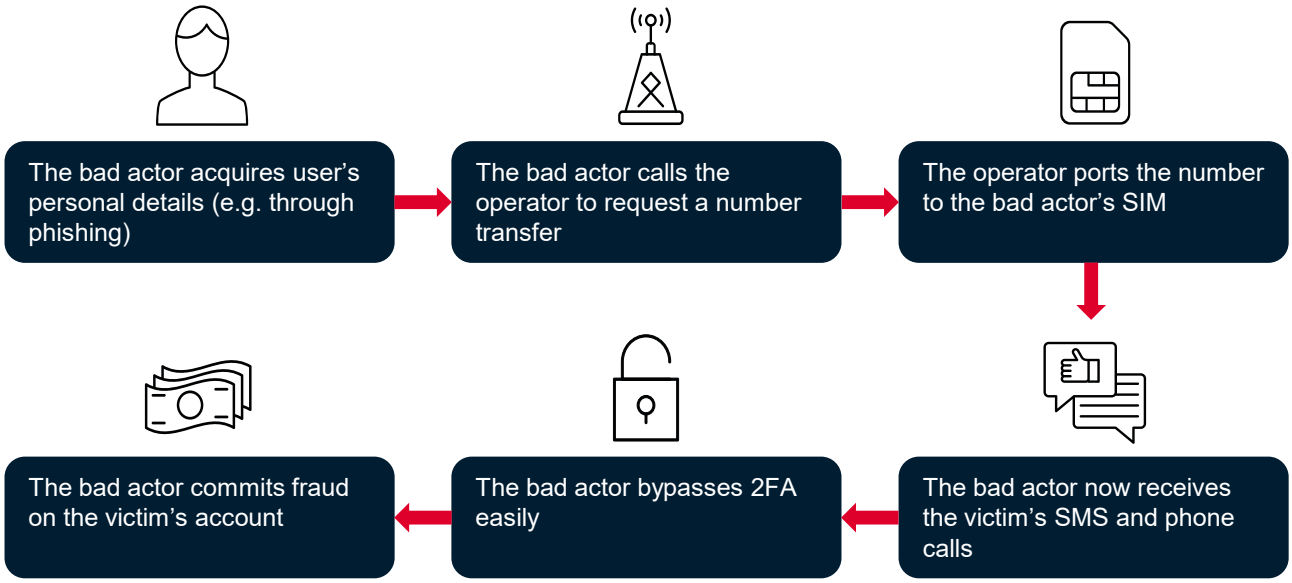
Source: World Economic Forum Global Risks Perception Survey 2023–2024



SIM swap is another example of an online threat; there has been a significant rise in the number of such cases in Asia Pacific and around the world in recent years. SIM Swap occurs when a fraudster manipulates the customer service process to take over an open account within a mobile operator. The fraudster does this by requesting a SIM replacement or initiating an MSISDN porting order, enabling them to intercept SMS on a device that they own. The fraudster can then take advantage of using two-factor authentication (2FA) to perform banking fraud, access mobile money accounts and gain control of other third-party accounts. (see Figure 3).

Figure 3: How SIM swap works

Source: GSMA Intelligence



In Asia Pacific, victims of SIM swap in several countries, including Australia, India, Japan and Vietnam, have reported losing significant amounts of money and having their privacy violated. In Thailand, over 10,000 illegal SIM cards were seized in crackdowns in 2022, many of which were registered with the identities of foreigners.[2] Elsewhere, the FBI recorded 1,650 cases of SIM swap in the US in 2021, resulting in losses of around $86 million,[3] while Europol dismantled criminal networks believed to have stolen personal information and more than $100 million through SIM swapping across Europe in the same year.[4]

Other widespread threats include child sexual exploitation and abuse online, phishing emails and SMS messages and DDoS attacks:

- Insights from Disrupting Harm – a joint research project funded by Safe Online and carried out by Unicef Innocenti, ECPAT International and Interpol in 13 countries, including six in Asia Pacific (Cambodia, Indonesia, Malaysia, Philippines, Thailand and Vietnam) – found that every year up to 20% of children experience sexual exploitation and abuse online, many of them through social media platforms.[5]

- A recent report[6] from AAG-IT showed that an estimated 3.4 billion spam emails are sent every day. The report also estimated that a data breach that exposes 10 million records costs businesses $50 million on average and an attack that compromises 50 million records can cost as much as $392 million.

- A report[7] from StormWall showed that DDoS attacks in Asia Pacific (including China) rose by 38% year on year in the first half of 2023.

Table 1: Examples of online threats reported in Asia Pacific countries

Source: GSMA Intelligence

Country	Type of threat	Example
Australia	Privacy breach	In 2022, several companies, including telecoms operators, reported various data privacy breaches, with attackers getting access to the emails and personal details of millions of customers.[8]
Bangladesh	Harassment	The Cyber Crime Awareness Foundation reports that about 80% of women in Bangladesh face online violence on various social media platforms. Police headquarters data in Bangladesh also showed that over 17,000 allegations of cyber harassment were reported every year since the formation of the Police Cyber Support for Women in November 2020.[9]
India	Cyber crime	In India, 65,893 cases of cybercrime were registered in 2022, an increase of 24.4% over 2021. 64.8% related to fraud, while 5.5% and 5.2% were cases of sexual exploitation and harassment, respectively.[10]
Indonesia	Disinformation	In the run-up to the February 2024 general elections in Indonesia, the Ministry of Communication and Informatics disclosed that it was working with Meta to take down 454 pieces of fake content related to the election on Facebook.[11]
Japan	Phishing	According to the Council of Anti-Phishing Japan, the number of phishing reports in 2022 reached 968,832, which was 17 times the number recorded in 2019.[12]
Malaysia	Phone scam	According to Gogolook's 2022 Annual Fraud Report, 73% of phone numbers belonging to more than 21 million people in Malaysia have been leaked or sold to scammers.[13]
Philippines	OTT text scam	Globe Telecom revealed that criminal groups use foreign SIMs and over-the-top apps to target their potential victims without getting tracked by authorities, as the numbers used fall outside the scope of the SIM Registration Act.
South Korea	Hacking	South Korea's National Intelligence Service reported that in 2022, the country was hit by a daily average of 1.2 million hacking attempts.[14]
Thailand	SMS scam	The Cyber Crime Investigations Bureau (CCIB) in Thailand disclosed that victims of SMS scams lost around THB174.15 million ($4.9 million) to SMS scammers who drove vehicles equipped with cell-site simulators, also known as stingrays, between March and May 2023.[15]

2. The impact of AI on online safety

AI has risen to the top of the agenda for digital industry players, and for good reason, as AI will have wide-reaching impacts across society, with the potential to drive positive change for people and businesses in every sector. At the same time, warnings have been issued on the risks associated with the misuse and/or unethical use of AI, resulting in increased scrutiny of the development and application of AI tools. Meanwhile, the launch of genAI platforms (such as OpenAI's ChatGPT and Google's Gemini), along with the ongoing integration of AI tools into smartphones and other end-user devices, has led to the democratisation of AI.

AI presents opportunities and risks for online safety almost in equal measure. As a force for good, AI's capabilities make it an ideal tool for identifying and preventing online threats. However, the technology could also allow bad actors to perpetuate online threats by making it harder to track cyberattacks (see Table 2).

Table 2: The two sides of AI in the online threat space

Source: GSMA Intelligence

AI as a force for good	AI as a tool in the hands of bad actors
Analyse large volumes of data to spot abnormalities and detect patterns	Create socially engineered emails, messages and images to bait victims
Detect inappropriate content on social media and automatically delete them	Use deepfakes as 'clickbait' to drive traffic to malicious websites
Predict future cyberattacks and identify vulnerabilities in the system	Increase fraud volumes and make them harder to detect
Catalyse instant response to incidents	Create voice clones for impersonation
Identify and mitigate threats from sophisticated malware	Create media content to spread misinformation and disinformation
Filter and remove child sexual exploitation and abuse material from the internet, including photos and videos	Create fake social media accounts and generate fake child sexual abuse material to target children and other vulnerable persons
Moderate chatrooms and other real-time online platforms to prevent inappropriate conversations between adults and minors	Identify weaknesses in online security measures, making it easier to access personal data

The consensus among security agencies is that AI will drive an increase in the volume and sophistication of online threats. For example, this includes the following agencies in Asia Pacific:

- The Association of Southeast Asian Nations' (ASEAN) Cybersecurity and Information Centre of Excellence has expressed concern over how bad actors could use AI tools such as ChatGPT to create highly convincing emails without the key indicators of phishing attacks. However, they also highlighted the opportunity to use the power of genAI to respond to the threat on an equal footing with cybercriminals.[16]

- The director of Singapore's National Cyber Threat Analysis Centre has disclosed that bad actors in underground forums were actively talking about "jailbreaking AI tools, such as

ChatGPT, to unlock their full malicious potential", a situation that could "put the capability to create ransomware using AI in the hands of each and every person" if they succeeded.[17]

- Unauthorised money transfers via internet banking in Japan rose by 16 times in the first six months of 2023, resulting in losses of around JPY3 billion ($21 million), according to the National Police Agency in Japan.[18] The increase is partly attributable to AI-enabled threats.

- South Korea's Ministry of Science and ICT and the Korea Internet & Security Agency have identified AI as one of the biggest cyber threats facing the country in 2024. Both agencies predict an increase in hacking attempts from "ordinary people" who do not have cybersecurity expertise, but could leverage genAI to create malicious codes, detect security flaws, draft convincing phishing emails and distort audio to fool intended victims.[19]

Elsewhere, the UK's National Cyber Security Centre has said that AI will almost certainly increase the volume and impact of cyberattacks in the period to 2025, owing to several factors. These factors include the lower barriers for novice cybercriminals to carry out effective attacks and the increased ability of bad actors to analyse exfiltrated data faster and use them to train AI models.[20]

However, government and industry leaders are exploring ways to leverage AI capabilities against online threats. Japan's Ministry of Defence plans to invest JPY25.6 billion ($237 million) to develop an AI system that can detect malicious emails and eventually neutralise the effect of attacks on public- and private-sector targets.[21] Malaysia's Communications and Digital Minister has suggested that AI can be utilised to cover the current shortage of expert manpower in the field of cybersecurity.[22] And a study published in November 2023 found that more than 80% of banks and payment service providers surveyed in Australia, Malaysia, the Philippines, Thailand and Singapore now use some form of AI to detect fraud.[23]

The need to address ethical concerns in the application of AI

The application of AI tools in efforts to tackle online threats raises important considerations around privacy and ethics. AI algorithms can sometimes reflect the biases of their developers or the data they are trained on, leading to discriminatory outcomes. This can have serious consequences in the context of online threats, resulting in false positives or false negatives. As such, authorities and industry stakeholders need to put in place the right governance frameworks to assess the development and application of AI systems to tackle online threats.

Authorities need to carefully balance AI's immense potential to tackle online threats with the necessary steps to mitigate the attempts of bad actors to use AI for distrustful purposes, in addition to considering the need to protect user privacy and maintain ethical boundaries. The GSMA's AI Ethics Playbook is intended to be a practical tool to help governments and organisations to consider how to design, develop and deploy AI systems in a responsible way. It is also designed to support organisations with varying levels of maturity in terms of AI adoption and familiarity with ethical principles.

3. Measures to improve trust in the digital age

The rapid expansion of the digital world means that societies are more dependent on digital services today than ever. Critical sectors – such as transport, health, public safety, emergency services and finance – rely on telecoms networks, particularly mobile, to deliver life-enhancing services. This is against a backdrop of an ever-increasing and continually evolving online threat landscape that is capable of eroding trust in digital services. Consequently, the need to address the diverse and increasingly prevalent threats that people and businesses face online has become a priority for policymakers and other stakeholders as part of efforts to build inclusive digital nations.

Several stakeholders have an interest in ensuring online safety and preserving trust in the digital world. These include governments, mobile operators (and other communication service providers), social media platforms and citizens (people and businesses).

This section evaluates some of the initiatives and measures to improve online safety in Asia Pacific. It is important to note, however, that online safety must be viewed as a shared responsibility between these stakeholders, as opposed to the sole responsibility of any single stakeholder. This highlights the need for open dialogue and cooperation between all parties in the digital ecosystem.

3.1 Governments

The socioeconomic damage and national security risks from online threats are significant: the global cost of cybercrime is expected to reach $23.84 trillion by 2027, up from $8.44 trillion in 2022.[24] Countries in Asia Pacific have reported considerable losses to cybercrimes. For example, data from Thailand's CCIB shows that cyberattacks led to losses of up to THB20 billion ($564 million) in 2023,[25] while Indonesia's National Cyber and Encryption Agency reported losses of IDR14.5 trillion ($920 million) in 2022.[26]

In Asia Pacific, governments have introduced several measures to improve online safety and build trust. It is worth noting, however, that some measures place additional cost and administrative burdens on operators. Also, some measures could potentially result in unintended consequences. For example, excessive regulations around application-to-person messaging could restrict its use and, by extension, impact operators' SMS revenues, while network shutdowns, such as during elections, may deny citizens of their human rights as well as access to life-saving services, including emergency and vital information services.

Governments have as much interest in protecting people and businesses in the digital world as they do in the physical. However, it is essential to assess the impact of these measures against clearly defined costs, benefits and risks to other stakeholders and wider society. It is also essential to consider the impact of any proposed measures on trust in digital services, especially where they

inadvertently limit the ability of service providers to keep people and businesses connected, such as data protection regulations that could constrain innovation and impact the scalability and flexibility required to realise digital nation ambitions.

Strengthening the resilience and security of telecoms networks

Telecoms networks, particularly mobile, are the primary gateway to the digital world. This applies especially in a digital nation, where advanced mobile networks such as 5G (and soon 6G) enable the integration of digital technologies into various sector of the economy. Considering the importance of telecoms networks to maintaining trust in digital services and extending the benefits of connectivity to all citizens, there is a growing emphasis on strengthening the sector's resilience and security. Examples of this include the following:

- The Australian government plans to class telecoms as 'critical infrastructure' under the Security for Critical Infrastructure Act,[27] a move that will heighten the cybersecurity requirements currently placed on the sector and introduce regular reporting requirements to show compliance.

- The Pakistan Telecommunication Authority has officially launched the National Telecom Cyber Security Strategy 2023–2028, an initiative to ensure the security and resilience of the telecoms sector and address the challenges posed by the increasing interconnectivity of telecoms networks and various online threats.[28]

Scanning messages for online threats

Mobile operators provide the connectivity that powers online communities, acting as the transport layer for content, and are subject to strict laws on the confidentiality of communications. However, in a bid to tackle online threats, some governments have recently initiated plans to allow operators to filter certain messages sent over their systems, such as in Japan and Singapore:

- In March 2023, it was reported that the Japanese government planned to exempt operators from a law that barred them from viewing the contents of communications sent over their systems in a bid to tackle the sources of cyberattacks. If approved, the exemption could be made in 2024, paving the way for operators to report serious attacks to the government.[29]

- Singapore has taken a multi-layered approach to address SMS scams, including a requirement for operators to implement SMS anti-scam filtering solutions. This involves the automatic scanning of SMS messages sent over operators' mobile networks for malicious links and the detection of keywords, phrases and formats typical of fraudulent messages.[30]

While this practice already exists in several markets across Asia Pacific and globally, there are concerns about the implications for user privacy. Without a high standard of privacy and confidentiality, consumers would find it hard to trust in the communications networks they use. For operators, this means implementing systems that can adequately decipher what is potentially fraudulent and what is not, ensuring that sensitive subscriber data and message contents never

leak outside of their network**.** It also means accounting for the additional costs required to implement and maintain such systems.

Regulating SIM swaps

SIM swap fraud **is** especially difficult to detect considering that the vast majority of SIM swap requests are legitimate and mobile operators risk frustrating customers who are genuinely seeking assistance because of the relatively small number of fraudulent requests. However, some regulatory measures have been proposed to curb the incidence of SIM swap fraud**,** such as the following:

- The Telecom Regulatory Authority of India has proposed changes to the mobile number portability rules to curb SIM swap fraud. First, operators will be required to suspend a porting request if it is coming from a number that has undergone a SIM swap in the previous 10 days. Second, a porting operator will be need to match the customer's details from the donor operator,[31] though the complexity of implementation of this requirement has raised concerns.

- The Australian Communications and Media Authority has implemented rules requiring mobile operators to perform stronger customer identity checks for high-risk transactions such as SIM swap requests, changes to accounts or disclosure of personal information.

Introducing online safety rules

Through legislation and other state instruments, some governments have introduced rules that place the responsibility for keeping people, especially children and other vulnerable groups, safe online on social media companies and other online platform providers. Such regulations often define how to handle ‘legal but harmful’ content (content that is not explicitly illegal but which, individually or in aggregate, poses a risk e.g healthcare or political misinformation) and outrightly illegal content, such as child sexual exploitation and abuse materials or content promoting violence against women or vulnerable groups. Some recent examples of online safety rules introduced in Asia Pacific include the following:

- In December 2023, the Australian government announced the Consolidated Industry Codes of Practice for the Online Industry to tackle child sexual exploitation and abuse online, pro-terror material, drug-related content and other harmful materials. The aim is to establish safer online experiences for citizens. The codes will be enforced by the Office of the eSafety Commissioner.[32]

- In July 2023, the government of Singapore issued a Code of Practice on Online Safety, which empowers the Infocomm Media Development Authority (IMDA) to designate social media companies that must comply with obligations to mitigate the risks from harmful content (e.g. child sexual abuse material, cyberbullying, self-harm). Designated companies include Facebook, HardwareZone, Instagram, TikTok, X and YouTube.[33]

- In December 2022, Thailand’s government published a decree that requires internet service providers to comply with content takedown requests within 24 hours. An impact report several months later found a high compliance rate among social media companies, although there is still opposition from civil society groups.[34]

- The Anti-Online Sexual Abuse of Exploitation of Children law came into effect in the Philippines in July 2022. The law enables the government to work with the private sector, including social media companies, to block child sexual exploitation and abuse online and put in place practical safeguards to prevent or detect recruitment and trafficking.[35]

While there has been broad political consensus for these rules, some critics have highlighted concerns around privacy and potential infringement on free speech, as well as the burden it places on online platforms to police content on their sites. For governments and industry players, it is essential to find the right balance between maintaining democratic rights and online safety.

Facilitating regional and cross-sector collaboration

Online threats transcend national boundaries and have the potential to impact different players within the digital ecosystem. As such, the implementation of a multi-stakeholder approach, which enables information sharing and the pooling of resources, can be an effective way to improve online safety. Collaboration could be between nations with a common interest or between companies from different sectors within national borders.

In Asia Pacific, ASEAN provides a platform for regional cooperation on online safety. In November 2022, the association organised the ASEAN ICT Forum on Child Online Protection in Cambodia to facilitate regional collaboration on online safety for children. In February 2024, a meeting of Digital Ministers of ASEAN nations endorsed the establishment of the ASEAN Working Group on Anti-Online Scam as a platform for member states to cooperate and collaborate on capacity building, training and sharing of information related to combating scams online and across digital and telecommunications channels.[36]

At the national level, some governments have taken steps to facilitate collaboration between key players in the digital ecosystem to fight online threats. For example, the Thai government, with the support of Unicef, formed a public-private partnership with mobile operators to launch the Thailand Safe Internet Coalition, an initiative to create a safer digital environment for children and young people.

In Singapore, the Monetary Authority of Singapore and the IMDA jointly proposed a shared responsibility framework for phishing scams, with specific responsibilities and incentives for financial institutions and telecoms operators to mitigate online attacks. Under the proposal, operators will provide a line of defence to filter potentially fraudulent SMS messages. With the focus of this proposal solely on SMS rather than including all messaging services, it could have unintended consequences and accelerate the use of other platforms and services for fraudulent activities, leaving citizens still exposed to harm. To avoid these unintended consequences, it is essential for regulators to take a uniform approach for all digital services and platform providers.

Establishing online safety helplines

For victims of online threats, knowing where to find help or redress is an important stage in the recovery process. As such, the move by some governments to launch helplines and interactive portals to provide necessary support to victims of various online threats is a step in the right direction. This includes the following examples:

- Thailand's anti-cybercrime operation set up the Anti-Online Crimes 1441 centre, a hotline that allows victims to freeze their bank accounts within 15 minutes. The centre is a collaboration between the Ministry of Digital Economy and Society, the Anti-Money Laundering Office, the Cyber Crime Investigation Bureau, the Bank of Thailand, the Thai Bankers Association, the Department of Special Investigation and the National Broadcasting and Telecommunication Commission, among other relevant agencies.[37]

- The Vietnam Network for Child Online Protection launched a website for protecting children online. The website provides information about child safety online and software developed for keeping children safe online. It also provides the ability to report child abuse online and to contact the Child Affairs Department's hotline.[38]

3.1 Mobile operators

Mobile operators are in a unique position in the online threat landscape, considering that they must deal with multiple issues simultaneously. First, operators have a responsibility to build and maintain resilient telecoms infrastructure that can withstand extreme conditions, including increased volumes of traffic and changes in usage patterns. This is fundamental to sustaining communications, especially during crises and emergency situations. This was recently demonstrated in Australia, where Optus disclosed that nearly 2,700 calls to emergency services were attempted during a 12–13 hour network outage on 8 November 2023.[39]

Second, operators have a responsibility to secure their networks from various forms of online threats. The telecoms sector is a common target for increasingly sophisticated cyberattacks on network infrastructure and services by bad actors looking to commit fraud or disrupt services, especially as they gain a better understanding of mobile network technology. At the same time, operators have the responsibility to protect their customers from fraudulent activities, ensure their privacy and the confidentiality of their communications, and safeguard other digital market participants from the activities of criminals looking to use their networks and services as a gateway to the digital world.

In an increasingly connected world, the consequences of online threats for operators could be significant. Fundamentally, they can damage consumer confidence and trust and long-term customer relationships. For example, a survey of mobile customers in Australia following a series of data breaches in 2022 found that the majority of respondents did not trust any operator and in some cases distrusted all operators.[40]

Online threats can lead to considerable financial losses for operators, both in the form of lost revenues due to cyberattacks on their networks and services and in the form of penalties (fines

and reimbursements) for crimes perpetuated on their networks. Examples of such financial losses include the following:

- Insights from the Communications Fraud Control Association's global telecoms industry survey showed a 12% increase in fraud losses in 2023, compared to 2021. This equated to around $38.95 billion lost in 2023, representing 2.5% of telecoms revenues.[41]

- Thailand's National Broadcasting and Telecommunications Commission plans to fine operators THB1 million ($28,000) a day if they fail to follow new SIM registration rules aimed at curbing SIM swap fraud.[42]

- NTT Docomo disclosed that it fully compensated the victims of a phishing scam that targeted around 1,200 customers and resulted in losses of about JPY100 million ($680,000).[43]

While customer trust is a function of multiple factors, supporting online safety is imperative for operators. Across Asia Pacific and beyond**,** operators have introduced measures to improve online safety. Some of these measures are highlighted in Table 3.

Table 3: Examples of operator online safety measures

Source: GSMA Intelligence

Online safety measure	Example
Scan SMS to filter and block fraudulent content	Globe blocked 2.2 billion scam and spam messages from international and domestic sources between January and June 2023.[44] Telstra blocked 225 million messages containing various forms of online scams between April and December 2022.[45]
Block access to child sexual exploitation and abuse materials to protect children online	One New Zealand has begun blocking illegal child sexual exploitation and abuse materials online after signing up to the Department of Internal Affairs' Voluntary Principles in June 2023.[46]
Verify customer identities to detect and prevent fraudulent activities	Airtel launched Airtel Safe Pay to protect customers from fraud while making online payments. The solution uses a combination of 2FA and one-time passwords to ensure that only the authorised user can complete a transaction.
Utilise AI and machine learning to enhance fraud detection capabilities	Singtel offers a network security solution, Broadband Protect, which uses AI and machine learning to identify and blocks malicious websites. Customers are alerted of potentially malicious webpages and can choose to unblock them using their My Singtel App if it is a trusted web link.
Collaborate to improve network resilience	Telkom Indonesia and Indosat Ooredoo Hutchison have teamed up to fortify digital infrastructure by establishing an interconnected internet exchange ecosystem and deploying a distributed security architecture.[47]
Alert customers when new threats emerge	In 2022, Reliance Jio emailed customers to warn them about e-KYC scams. The email provided details about the scam and how customers can avoid falling victim to them.
Offer malware protection for safer internet browsing	In 2022, Dtac launched Dtac Safe, a value-added cybersecurity service, to protect its customers. The solution is integrated as a

	software development kit within Dtac's existing app to protect users while they browse online.
Provide technical support for vulnerable users	Japanese operators NTT East and NTT West have introduced free call display services for the elderly to combat 'special fraud' scams. In 2022, there were 17,520 cases of special fraud across Japan, with total damages amounting to JPY36.1 billion ($243 million).[48]

Beyond these efforts, operators have an opportunity to work collaboratively to mitigate new and existing risks and, by extension, enhance online safety and consumer trust. The GSMA, through various initiatives, provides a platform for operators to leverage in the fight against online threats. These include the following:

- The Mobile Alliance to combat Digital Child Sexual Exploitation brings together operators committed to working together to fight technology-facilitated child sexual exploitation.
- The GSMA Open Gateway initiative has several network APIs that can help operators improve online safety, such as Sim Swap and One-Time Password SMS.
- The GSMA Fraud and Security Services provides the tools needed to take swift action against the most prevalent online threats that have been identified by the GSMA's Fraud and Security Group (FASG).

3.3 Social media platforms

Social media companies have transformed the way people create and consume information and entertainment. They have democratised knowledge sharing and broadcasting, while the network effect of their platforms means that digital content shared in various formats, such as videos, podcasts, and blogs, can potentially reach a global audience. Today, more than three out of five people in the world use social media. The daily average usage reached 2.5 hours in 2023, nearly an hour more compared to a decade earlier.[49] These figures are even higher among Generation Z,[i] who are also less reliant on traditional media compared to older generations.

The growing influence of social media and the relatively low entry barrier for content creators have made it a potent tool for bad actors to spread harmful content, such as misinformation and disinformation on a variety of sensitive topics (e.g politics, religion and health), child sexual exploitation and abuse materials, and hateful content targeted at a particular group or individual. Meanwhile, the advent of genAI could exacerbate the impact of social media–based online threats through large language models (LLMs) that can proliferate deepfakes and chatbots, which can craft and rapidly disseminate false information. According to a recent estimate, more than 15 billion images were created using text-to-image algorithms between 2022 and 2023.[50]

[i] People born between the mid-1990s and mid-2010s.

The potential for malicious content can ruin the otherwise positive experience that people can get on social media and the internet more broadly. This highlights the scale of the responsibility of social media companies and other platform providers to take concrete steps to improve online safety and build trust. While regulations, such as online safety bills introduced by some governments, have a role to play, there is a case for social media companies to use internal mechanisms to address the growing concerns over the spread of harmful content on their platforms.

In recognition of this responsibility, some social media companies have recently announced measures to improve online safety globally as well as in specific markets across Asia Pacific. In February 2024, for example, Meta took a significant step in this direction by announcing several measures to curb the spread of false information on Facebook, Instagram and Threads. These include building tools to detect, identify and label AI-generated images shared on these platforms, developing LLMs to automatically moderate content online and collaborating with industry partners on common technical standards for identifying AI-generated content.[51]

Meta has also announced country-specific measures. For example, Meta has collaborated with the RATI Foundation in India to launch Meri Trustline, a helpline dedicated to supporting children under the age of 18 years who are facing online safety concerns, such as cyberbullying and child sexual exploitation and abuse. The company has also partnered with Brac in Bangladesh to reach 10 million women and teenagers and is collaborating with organisations such as Zindegi Trust in Pakistan to promote online safety among vulnerable people.

Google has also announced a number of steps to improve online safety, including $1.2 million in funding to support CekFakta – a collaborative fact-checking project initiated by the Indonesian Anti-Defamation Society, the Alliance of Independent Journalists and the Indonesian Cyber Media Association – to fight misinformation ahead of the 2024 Indonesian election. Google also displays information panels on YouTube to give topical context for users in Singapore, Pakistan, Papua New Guinea and New Zealand, and provides an educational programme called Hit Pause in several countries, including India, Indonesia, Australia and New Zealand, to encourage users to think critically about information.[52]

For its part, Tik Tok launched an Asia Pacific Safety Advisory Council in 2020, bringing together thought leaders from academia, law and government to provide subject matter expertise and advise on TikTok's content moderation policies and practices to improve online safety. In 2022, the company launched a campaign in South Korea to keep teenagers safe online and reiterated various safety measures such as removing inappropriate content, setting a minimum age of 14 years and restricting public access to content posted by users under the age of 16 unless the uploader gives their permission.[53]

Despite these measures, there are still concerns over online safety on social media platforms. Other stakeholders have highlighted issues that still need to be addressed, considering the increasing sophistication of online threats and the need to protect vulnerable people on online.

For example, a report by Ofcom, the UK telecoms regulator, showed that a third of children aged between 8 and 17 with a social media profile have been able to sign up with an adult-user age by providing a false date of birth.[54] This increases the risk of these children being exposed to inappropriate content on social media platforms. Security agencies and civil society have also raised concerns about the potential for the end-to-end encryption feature on many social media platforms to impede the fight against child sexual exploitation and abuse online.[55]

The 2024 Edelman Trust Barometer showed that the social media industry is the least trusted (out of 17 industries) by customers to do what is right.[56] This should serve as a wake-up call to social media companies on the need to do more to improve online safety. In practice, this should involve continuous engagement and collaboration with other stakeholders, including mobile operators, to track new online threats and their intended targets and to find effective ways to support victims and protect other vulnerable users.

3.4 Citizens

Digital service customers are usually the primary target of online threats. Telenor Asia's Digital Lives Decoded 2023 study, which surveyed over 8,000 mobile internet users across eight countries,[ii] found that the majority (90%) of respondents shared concerns on privacy and security.[57] A number of factors could increase the vulnerability of certain customers. These include digital skills gaps that limit their ability to identify or mitigate online threats, personal features (e.g age or gender) that make them the target of online abuse and harassment and breaches of their personal information (e.g contact details) that expose them to perpetuators.

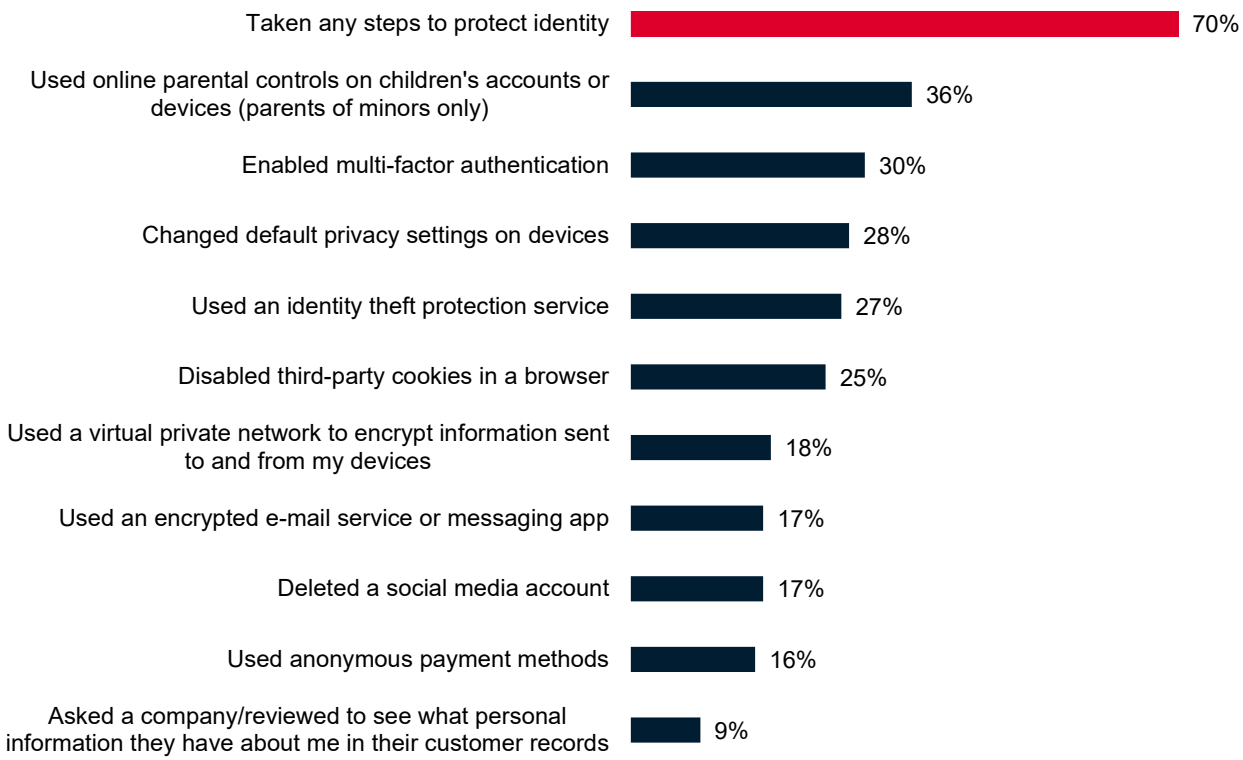
As highlighted above, governments, mobile operators, social media companies and other stakeholders do have enormous responsibility to protect customers online, such as through policies and technical solutions to prevent online threats. However, customers also have a responsibility to take certain measures to stay safe and keep others safe online, especially considering that the effectiveness of some of the measures introduced by other stakeholders depend on the complementary effort of customers.

The majority (70%) of respondents to a recent survey indicated that they have taken steps protect their identity online, with a much lower share having taken additional steps (see Figure 4).

[ii] Bangladesh, Indonesia, Malaysia, Pakistan, the Philippines, Singapore, Thailand and Vietnam

Figure 4: Measures taken by customers to protect personal information, January 2023
Percentage of respondents

Source: Statista



Clearly, a sizeable number of customers are not yet taking any measures to protect themselves online. The likely reasons include ignorance of the prevailing risks in the digital world, lack of awareness of the possible measures to stay safe online or the required digital skills to implement those measures, and overconfidence in the security measures put in place by their service provider (e.g mobile operator or social media company) to keep them safe. This scenario is risky and unsustainable, and highlights the need for concerted efforts by governments and digital ecosystem players, supported by civil society and other interest groups, to help customers implement necessary measures to stay safe online.

4. Action points to improve online safety and trust

Stakeholders across Asia Pacific have introduced various measures to improve online safety, some more than others. But for everyone it is a race against time, considering the ever-increasing and evolving scope of the online threat landscape. Here, we highlight five steps to support existing measures and inspire new ones:

- **Awareness:** Various stakeholders offer tools on online safety, but many citizens may not be aware of them or aware of how to access those tools. Meanwhile, the online threat landscape is changing rapidly with the emergence of AI-driven threats that are more difficult to detect. This has the potential to widen an already significant awareness gap among customers on the risks they face online. Stakeholders should therefore take steps to create more awareness around online threats and solutions, such as by signposting technical tools (e.g. 'parental controls' and anti-malware software) to stay safe online.

- **Education**: Beyond awareness of various online threats, people and businesses need to be equipped with 'digital resilience' skills (knowledge of how to navigate and respond to risks) to help them become confident digital citizens. This may involve simple steps around protecting accounts with 2FA or how to react to SMS and emails from suspicious sources. It may also involve collaborating with parenting groups, educators and other organisations that work with children to help amplify the messaging on safe and responsible online behaviours.

- **Collaboration**: The digital ecosystem comprises many different players whose services are either conduits for cyberattacks on their customers or are themselves targets of some forms of cyberattacks. This suggests a common interest in improving online safety. Collaboration within and across industries is essential to achieving this objective. This can be achieved by facilitating information sharing, resource pooling and efforts to take a common approach in tacking various threats. Furthermore, the criminal nature of some online threats also means that ecosystem players would have to collaborate with law enforcement agencies.

- **AI opportunity**: To ensure online safety, stakeholders must stay at least one step ahead of the bad actors. In the emerging AI era, it has become an imperative for stakeholders to take advantage of the opportunity that AI presents, not only to mitigate existing online threats but, perhaps more importantly, also to counter new, more sophisticated threats that are driven by AI. Policymakers have a role to play by implementing AI frameworks that support positive innovation, along with safeguards to prevent the misuse of AI for various forms of online threats.

- **International cooperation**: Online threats often transcend geographical boundaries and local jurisdictions, such as online child sexual exploitation and abuse crimes that are perpetuated over social media and other internet platforms. Regional and global cooperation is required to prevent such threats. In Asia Pacific, regional platforms, such as ASEAN, provide an opportunity for member states to exchange ideas on how to tackle online crimes and share information that can help identify perpetuators. Beyond regional bodies, countries can also take advantage of bilateral and multilateral relationships with partners in other regions to improve online safety.

The benefits of participating in the digital world for people and businesses are not in doubt. This is the premise for the increasing focus on digital nationhood by governments in Asia Pacific and beyond. However, online threats could undermine those ambitions by eroding trust in digital services and goodwill towards service providers, such as mobile operators and social media companies, whom customers expect to keep them safe online. For stakeholders in the digital ecosystem, there’s no better time than now to work together to improve online safety for citizens in order to build trust and inclusivity, and realise ambitious digital nation goals.

References

[1] The Global Risks Report 2024, World Economic Forum, 2024

[2] “Illegal SIM cards 'integral' to scams”, Bangkok Post, March 2022

[3] “FBI Las Vegas Federal Fact Friday: SIM Card Swapping”, FBI Las Vegas, October 2022

[4] “SIM swapping: 10 arrested in Europe over €82.4m scam to hijack celebrities' phones”, Euronews, February 2021

[5] https://safeonline.global/disrupting-harm/

[6] https://aag-it.com/the-latest-phishing-statistics/

[7] "Multi-vector DDoS attacks up by 117% in H1 2023", CybersecAsia, August 2023

[8] "Australia Inc roiled by string of cyber attacks since late 2022", Reuters, December 2023

[9] "Govt must ensure online safety for women", New Age, December 2023

[10] "Crimes against women, children, SC/ST, and cyber crimes, increased in 2022: Crime in India report", The Hindu, December 2023

[11] "Fake news on Indonesia election spreading as govt asks Facebook to take down over 450 ‘hoaxes’", The Straits Times, November 2023

[12] "'SIM swap' phone hijacking scam in Japan used to steal money in as little as 15 min", The Mainichi, June 2023

[13] “Most cell phone numbers in Malaysia are leaked and sold to scammers. Are telcos to be blamed?”, Tech Wire Asia, April 2023

[14] https://www.trade.gov/market-intelligence/south-korea-cybersecurity#

[15] "SMS scam gang arrested", Bangkok Post, May 2023

[16] "Phishing Attacks Rise Sharply in Southeast Asia", BankInfoSecurity, July 2023

[17] "Hackers trying to corrupt AI, raising level of ransomware threat: S’pore cyber-security director", The Straits Times, October 2023

[18] "Record ¥3 billion stolen via phishing in Japan in first half of 2023", The Japan Times, August 2023

[19] "South Korea anticipates generative AI-powered attacks as prominent threat in 2024", The Readable, December 2023

[20] The near-term impact of AI on the cyber threat, National Cyber Security Centre, 2024

[21] "Japan to invest $237.12 million in Artificial Intelligence to counter Cyber Attacks", Cybersecurity Insiders, March 2020

[22] "Fahmi: AI technology can help overcome shortage of cyber security experts", Malay Mail, November 2023

[23] "New report finds that more than 80% of organizations across APAC are using artificial intelligence (AI) to tackle fraud", Feedzai, November 2023

[24] Statista

[25] "Cyber crime costs Thailand 6.76 billion baht in 70 days", Thaiger, January 2024

[26] "BSSN Records 361 Million Cyber Attacks in Indonesia", Tempo.co, November 2023

[27] "News reaction: Australian Government announces intention to extend SOCI to telecoms", NCC group, November 2023

[28] "‘Fortifying Telecom Sector’: PTA unveils cyber security strategy 2023-2028", Pakistan Today, December 2023

[29] "Japan to enlist telecom carriers in fight against cyberattacks", Nikkei Asia, March 2023

[30] https://www.imda.gov.sg/how-we-can-help/anti-scam-measures

[31] "TRAI proposes tweaks in MNP rules to curb SIM-swap frauds", Economic Times, September 2023

[32] https://www.esafety.gov.au/industry/codes/register-online-industry-codes-standards

[33] "IMDA's Online Safety Code comes into effect", IMDA, July 2023

[34] "Digital Rights in Thailand in 'Free Fall' Analysts Say", Voice of America, December 2023

[35] "Internet now safer for kids with anti-online sexual abuse law", Philippine News Agency, August 2022

[36] The 4th ASEAN Digital Ministers' Meeting and Related Meetings

[37] "Anti-online Scam Centre gets off the ground", Nation Thailand, November 2023

[38] "Vietnam launches website to keep children safe online", The Digital Watch, March 2022

[39] "2,700 Triple Zero calls failed during Optus outage", Information Age, January 2024

[40] "A majority of Australians have no trust in telcos", Roy Morgan, October 2022

[41] "Telecommunications fraud increased 12% in 2023 equating to an estimated $38.95 billion lost to fraud", CFCA, November 2023

[42] "Operators face huge fines over sim cards", Bangkok Post, September 2022

[43] "Docomo reports ¥100 million in damages in phishing scam", Japan Today, October 2021

[44] "Globe Blocks New Record High 2.2 B Spam, Scam SMS in H1", Globe, August 2023

[45] "We've blocked over 225 million scam text messages since April", Telstra, December 2022

[46] "One New Zealand tackles online child sexual exploitation and abuse", One New Zealand, June 2023

[47] "Telkom, Indosat seal internet exchange partnership", Mobile World Live, January 2024

[48] "Japan telecoms giants to offer 'call display' free to elderly to fight phone fraud", The Mainichi, March 2023

[49] Statista

[50] "AI Has Already Created As Many Images As Photographers Have Taken in 150 Years. Statistics for 2023", Everypixel Journal, August 2023

[51] "Labeling AI-Generated Images on Facebook, Instagram and Threads", Meta, February 2024

[52] "How we're fighting misinformation across Asia Pacific", Google Blog, March 2023

[53] "TikTok Korea launches campaign to keep teens safe online", Korea JoongAng Daily, March 2022

[54] "A third of children have false social media age of 18+", Ofcom, October 2022

[55] "Child protection organisations issue warning to social media companies about online safety", Barnardo's, January 2022

[56] 2024 Edelman Trust Barometer, Edelman, 2024

[57] Telenor Asia Digital Lives Decoded 2023, Telenor Asia, 2023

GSMA
Intelligence

gsmaintelligence.com