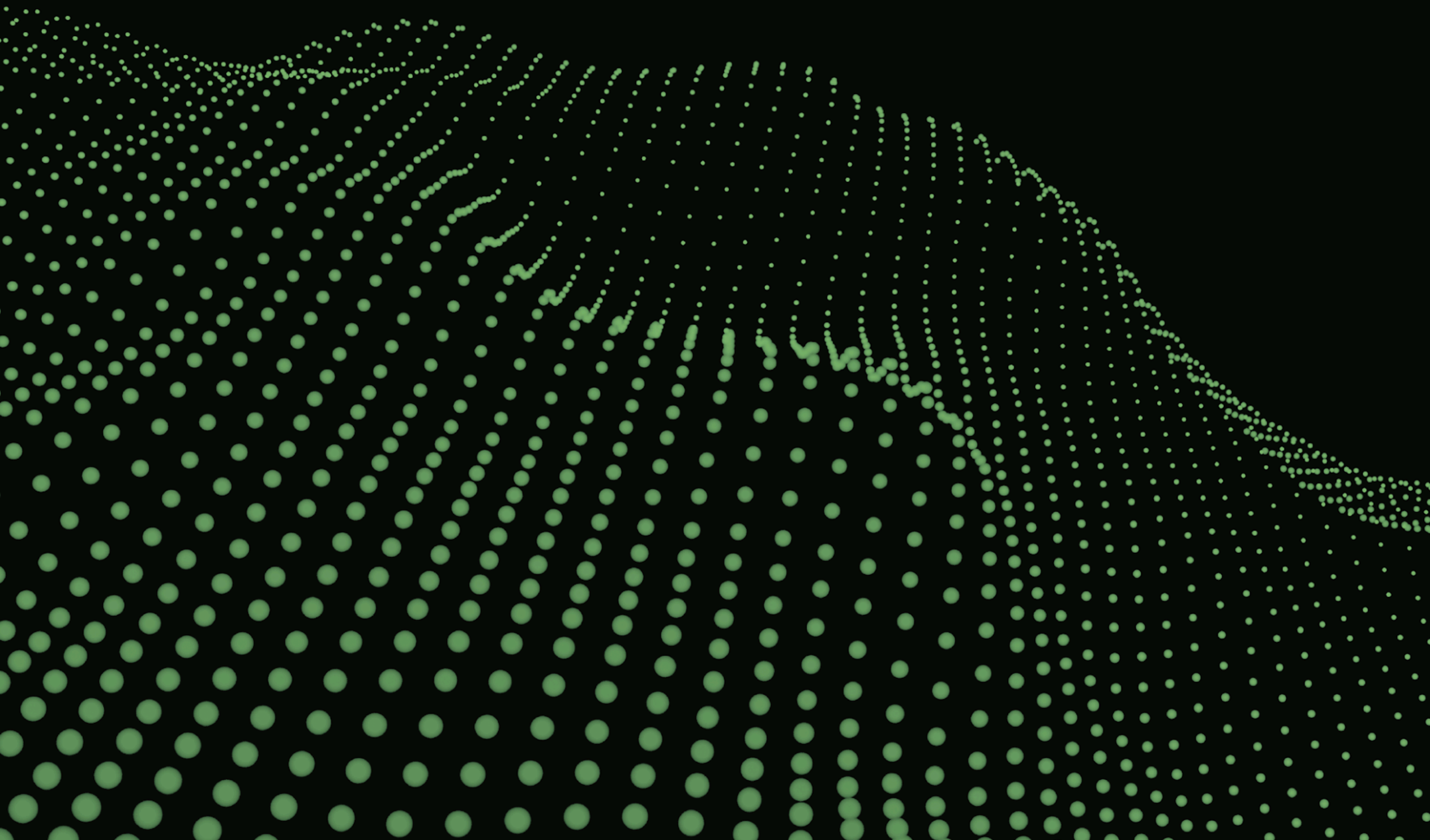
Australian Online Scams Code

A code of practice for the digital industry



Australian Online Scams Code

Executive summary for consumers

Under the Australian Online Scams Code, signatories agree to adopt the following measures, as detailed within the code:

- *Blocking*: Deploy measures to detect and block suspected scams.
- *Reporting*: Have a simple and quick route for users to report possible scams.
- *Takedowns*: Take quick action against verified scam content and scammers.
- *Advertising*: Deploy measures to protect people from scam advertising.
- *Email and messaging*: Deploy specific measures to protect people from scams in emails and private messages.
- *Law enforcement*: Engage with law enforcement efforts to address scams.
- *Intelligence sharing*: Contribute to public-private and cross-sectoral initiatives to address scams.
- *Communications*: Provide information about scam risks and support counter-scam efforts.
- *Future proofing*: Contribute to strategy development and future proofing exercises to stay ahead of the threat.

1. Background

1.1. Scams are a significant social and economic problem for Australians. Scams may be perpetrated using a wide range of techniques across a wide range of systems and industry sectors; Addressing the threat requires collaborative effort and must be a priority for all.

1.2. Scam activity can be sophisticated and hard to detect. It usually originates offshore, readily adapts to disruption measures and exploits new opportunities and vulnerabilities. Scammers perpetrate their crimes via a range of obfuscation techniques and scam types, across a range of digital and other services, including via telephone and SMS, banks and other financial services. An ecosystem approach should be adopted, with government, relevant agencies, industry and consumers all having a role to play.

1.3. The Australian Online Scams Code (AOSC) has been developed by the Digital Industry Group Inc. (DIGI), a non-profit industry association that advocates for the interests of the digital industry in Australia. It is a proactive initiative by DIGI and relevant members and other industry participants that sets out a series of commitments that digital service providers can make to help combat scams. The code reflects the desire of participants within the digital industry to work together to minimise the harm caused by scams in Australia.

1.4. Recognising the need for interoperability with global services, the AOSC is intended to be consistent with and build upon overseas frameworks.[1]

[1] DIGI wishes to acknowledge the work of TechUK in developing the UK Online Fraud Charter, a voluntary agreement between the UK Government and members of the technology sector in the UK to tackle the threat posed by scams and other online. See Home Office (30/11/2023), Online Fraud Charter, https://www.gov.uk/government/publications/online-fraud-charter-2023

1.5. The AOSC may be adopted by any digital service provider that is provided to Australian end-users in the categories identified in Section 4. Signatories of this code are not limited to those outlined; other digital service providers are encouraged by DIGI to agree to the actions enclosed to better protect their customers and the wider Australian public. The signatories to the AOSC are listed on the DIGI website. Companies may adopt the AOSC, and withdraw from it, by notifying DIGI in writing.

2. Guiding principles

2.1. The commitments are intended to be applied with consideration for the following guiding principles.

2.1.1. *Diversity of services:* The digital industry is highly diverse. The commitments set out in this Code are principles-based and intended to be flexible enough to account for the differing nature and sizes of Code signatories and complexity of their supply chains. This is to allow participating service providers to apply this code as appropriate to reflect the particular features of their services or business models, the nature of any scam activity on their services, and any other relevant circumstances.

2.1.2. *Proportionality*: Scams will vary greatly in incidence, scale and impact amongst the diverse range of services and products offered by different digital service providers. Accordingly, Signatories can take risk-based actions which are proportional responses to their commitments under the AOSC. In so doing, Signatories should give attention to the volume of dissemination, its financial impact and harm to Australians.

2.1.3. *Protection of user privacy:* Any actions taken by Signatories to address scams should not contravene commitments they have made to respect the privacy of users, including in terms and conditions, published policies and voluntary codes of conduct as well as by applicable laws.

2.1.4. *Protection of freedom of expression*: Digital service providers provide a vital avenue for the open exchange of opinion, speech, information, research and commerce across the Australian community. In implementing the AOSC, Signatories are encouraged to be cognisant of the need to balance freedom of opinion and expression, and the protection of a range of legitimate interactions and business activities of their users.

2.1.5. *Need for collaboration and cooperation among all relevant stakeholders:* Signatories recognise the range of stakeholders, including the diversified Signatories to this Code, that have a role to play in disrupting the scams ecosystem.

2.2. The commitments are not intended to require signatories to:

2.2.1. breach any law or mandatory code of practice by which they are bound;

2.2.2. do anything inconsistent with the applicable terms of use, policies or conduct rules that apply to their services;

2.2.3. take steps that are disproportionate to the threat presented by scam activity taking place on their services or otherwise unreasonable in context; or

2.2.4. interfere with legitimate and authorised use of their services.

3. Identifying scams

3.1. For the purposes of the AOSC, a scam is an invitation, request, notice or offer by a person with the purpose of deceiving another person in order to obtain a financial benefit or cause a financial loss.

3.2. Some common typologies of scams include:

3.2.1. *Investment scams*: Perpetrators offer lucrative investment opportunities to victims who are pressured into investing into a fictitious fund or service.

3.2.2. *Product and service scams:* Perpetrators sell products or services that are non-existent or that never arrive to victims.

3.2.3. *Romance scams:* Perpetrators manipulate victims into trusting them and believing they are in a genuine relationship, in order to pressure victims into sending money through emotive requests.

3.2.4. *Impersonation scams:* Perpetrators pretend to be a trusted figure, ranging from a celebrity or legitimate organisation such as a bank, to deceive victims into sending money.

3.2.5. *Extortion scams:* Perpetrators pretend to be from an organisation and claim victims need to pay money, threatening arrest, deportation, physical harm or sexual exploitation if payment is not made.

3.2.6. *Employment scams*: Perpetrators pretend to be hiring on behalf of companies and convince victims to provide account and identity details, which they use to steal their money.

3.2.7. *Phishing scams*: Perpetrators communicate with people to encourage them to provide personal information in a way that may lead to them being defrauded.

3.3. For the purposes of the AOSC, Digital Content that is harmful but not a scam of the sort addressed by the AOSC includes that which is:

3.3.1. Unauthorised fraud, such as cybercrimes that may use hacking, data breaches and identity theft, that do not involve the deception of a consumer into ‘authorising’ the fraud; and

3.3.2. Consumer disputes about misleading and deceptive practices relating to the sale of goods and services, other than where a seller profile or website is not legitimate.

4. Applicable digital service providers

4.1. Signatories will implement the commitments that apply to their service category, as noted alongside each commitment.

4.2. The AOSC is primarily designed for consumer services where there is two-way interaction between end-users, with at least one being an Australian end-user (being an end-user who is either ordinarily a resident in Australia or an Australian account holder), and is intended to apply to the following services:

4.2.1. *Social Media Services:* Electronic services with a sole or primary purpose of enabling online social interaction between end-users; and which allows end-users to link to, or interact with, some or all of the other end-users; and allows end-users to post material on the service.

4.2.2. *Social Media Services with Peer-to-Peer Marketplaces:* Social Media Services that offer a platform that connects people who own a product or offer a service with people who want to buy, rent or otherwise own it.

4.2.3. *Email Services:* Closed-communication electronic mail services with the sole or primary purpose to enable an end-user to send and receive communications with another end user, through web browsers or software. This does not include email marketing software designed for the one-way distribution of HTML and other emails.

4.2.4. *Messaging Services:* Services with the sole or primary purpose of enabling one-to-one or one-to-many message-based communication via text, images, video and voice.

Note 1: Messaging services do not include 1) enterprise services 2) messages that have been verified as part of another scheme (such as an SMS registration process) or are regulated as part of another scheme (such as SMS/MMS).

Note 2: Where another digital service defined in this section 4 of the AOSC includes a private messaging feature, the private messaging feature will for the purposes of the AOSC be treated as a separate Messaging Service under section 9, rather than as part of the other digital service.

4.2.5. *Video Sharing Services:* Electronic services with the sole or primary purpose of providing audio-visual user-generated content to end-users and which allows users to interact with that content.

4.3. Signatories recognise the importance of preventing the amplification of scams through paid advertising, so the AOSC contains specific commitments for:

4.3.1. *Paid Advertising Services on Digital Platforms:* Services provided by a Signatory to a buyer (i.e. an advertiser or agency) to enable the buyer to purchase advertising placements on 1) a Social Media Service or Video Sharing Service operated by the Signatory; or 2) a general search engine service operated by the Signatory. This refers to paid for digital advertising on a Signatory's owned and operated services, where the Signatory controls the relationship with the advertiser (or their agency) and the user.

Note: Other forms of content outside of Paid Advertising Services on Digital Platforms, such as marketing and sponsored content including paid arrangements between advertisers and influencers, are covered under the commitments relevant to the services outlined in 4.2.

4.4. The AOSC is not intended to apply to services that collate information, programs or services from a range of sources on the Internet. Therefore, the following services are not considered to be applicable: Music, audiobooks, podcasting services, content and news aggregation, content and streaming services primarily offering licensed, professional content, organic search results, app stores and retail marketplaces.

4.5. Where a Signatory offers multiple services, its commitment relates to the applicable services noted in Section 4.2 and/or 4.3.1.

4.6. Certain commitments are only intended to apply to, or are intended to exclude, certain types of services, as noted alongside the commitment.

Commitments

5. Blocking

Deploy measures to detect and block suspected scams.

5.1 to 5.4 apply to:
Social Media Services
Social Media Services with Peer-to-Peer Marketplaces
Video Sharing Services

5.1. Ensure scams are addressed in community standards, guidelines or terms of service as non-compliant activity.

5.2. Have, or adopt, and maintain effective internal processes to allow detection, flagging and removal of content and/or accounts that meet internal thresholds of suspicion of being a scam.

5.3. Have, or adopt, and maintain appropriate processes designed to block or terminate users for creating new accounts, when the original accounts have previously been removed for scams, excluding those who have had their accounts taken over.

5.4. Offer appropriate login authentication methods, and encourage users to adopt strong security measures, such as two-step verification.

5.5 and 5.6 applies to
Social Media Services with Peer-to-Peer Marketplaces

5.5. Provide guidance to users on how to stay safe when buying and selling items directly with other users.

5.6. Commit to and/or move towards introducing reasonable and targeted measures for the verification of users using the Signatory's peer-to-peer marketplaces.

6. Reporting

Have a simple and quick route to report possible scams.

6.1 to 6.4 apply to:
Social Media Services
Social Media Services with Peer-to-Peer Marketplaces
Video Sharing Services

6.1. Have, or adopt, and maintain a simple in-product mechanism for users to report suspected scam content.

6.2. Action user reports as swiftly as reasonably possible if the reported content meets internal thresholds of suspicion.

6.3. Have, or adopt, a simple and direct process for law enforcement and trusted government partners to quickly and easily report suspected scam activity occurring on the company's services.

6.4. Indicate to users that they may report scams to law enforcement and their bank.

6.5 applies to Social Media Services

6.5. Provide or develop appropriate protections, which may include displaying warnings or allowing users to control or block messages, where users are contacted, through direct messages, by unknown accounts or individuals who may be suspicious or present a risk of scams.

7. Takedowns

Take quick action against verified scam content and scammers.

7.1 to 7.3 applies to:
Social Media Services
Social Media Services with Peer-to-Peer Marketplaces
Video Sharing Services

7.1. Remove scam content expeditiously, once found by the Signatory to be contravening applicable terms of service or policies, unless in exceptional circumstances.

Note: Reported content that does not violate applicable terms of service or policies does not need to be removed. The aim will be to remove content within 24 hours of the content being determined to be part of a scam by the relevant digital service provider.

There will also be cases where, upon investigation of the report, the Signatory determines that the reported material does not meet their policy standard for removal. A service may ask for additional information to assist its inquiries. The questions it may ask will necessarily differ based on the service, and provide important checks and balances for services to appropriately consider the contextual circumstances of the material, and the implications of a takedown decision.

7.2. Take appropriate enforcement action expeditiously against users suspected of posting, sending or sharing scam content, once found to be contravening the Signatory's terms of service, unless in exceptional circumstances.

7.3. Have a clear process for users to request reinstatement of access to their account following an account takeover or scam, where practicable taking into account situations where linked recovery accounts have also been hacked.

8. Advertising

Deploy measures to protect people from scam advertising.

8.1 to 8.5 apply to Paid Advertising Services on Digital Platforms

8.1. Offer or develop verification or authentication measures for all new advertisers, appropriate to the particular service.

8.2. Commit to and/or move towards introducing reasonable measures to confirm that an advertiser holds the necessary financial services licence to advertise a regulated financial service.

8.3. Have or introduce measures to screen advertisements for suspicious content and scan embedded URLs to monitor if they change during the lifecycle of the advert.

8.4. As appropriate, deploy processes to combat URL cloaking (i.e. where bad actors hide a destination website's URL by redirecting it to another web page).

8.5. Commit to and/or move towards developing a simple scam reporting mechanism on Paid Advertising Services so users can easily access the reporting function.

9. Email and messaging

Deploy specific measures to protect people from scams in email and messaging.

9.3 to 9.6 apply to Messaging Services Email Services

9.1. Section 9 applies to Email Services or Messaging Services where the communication is received by an Australian account holder.

9.2. Many private messaging services are more private and secure than public communications. Often, these services employ technology like end-to-end encryption in order to keep people safe from harms like compromise of personal information. In order to put those protections in place, the types of measures that are appropriate for combatting scams will differ for private messaging services, compared to those services with public communication. Providers do not have the same level of visibility over content, data and context when compared to public services.

9.3. The obligations in Section 9 do not require a service provider to:

9.3.1. implement or build a systemic weakness, or a systemic vulnerability, into a form of encrypted service or other information security measure;

9.3.2. render methods of encryption less effective;

9.3.3. build a new decryption capability in relation to encrypted services;

9.3.4. undertake monitoring of private communications.

9.4. Service providers must make available guidance material for users on scams. Such guidance material may include the type of scams to which customers may be exposed and the steps users may take to mitigate those risks, including:

9.4.1. how to block senders of unwanted private communications;

9.4.2. advising on users contacting their financial institution immediately if they believe they may have fallen victim to a scam;

9.4.3. not responding to messages or emails from unknown senders, or following links provided by such senders, where the communication is not expected;

9.4.4. how to report incidents of scams to law enforcement or similar organisations (such as the NASC).

9.5. Service providers must ensure initiating scams is addressed in community standards, guidelines or terms of service as a breach of those standards, guidelines or terms of service.

9.6. Service providers must have systems or processes designed to:

9.6.1. monitor for and identify scams, to the extent reasonably possible. This could include, for example, monitoring behaviours indicative of scam communications;

9.6.2. as soon as reasonably practicable, take appropriate action in response to such behaviours; and

9.6.3. identify trending or changing behaviour associated with scams, which may include as a result of complaints received.

Note: Systems or processes designed to meet the obligations under Section 9 may include, for example, identifying and blocking bulk sending by newly established accounts, or monitoring complaints received from users regarding scams.

10. Law enforcement

Engage with law enforcement efforts to address scams.

10.1 to 10.3 apply to:
Social Media Services
Social Media Services with Peer-to-Peer Marketplaces
Email Services
Messaging Services
Video Sharing Services
Paid Advertising Services on Digital Platforms

10.1. Respond to valid Australian law enforcement requests under applicable legislation for user information as soon as reasonably practicable.

10.2. Respond to valid Australian law enforcement requests under applicable legislation to provide information, by due process, on persistent and prolific serious and organised crime actors targeting the Australian public, to support investigative and intelligence operations.

10.3. Consider other ways to support crime prevention, such as the provision of training, dedicated law enforcement reporting channels, or engaging in public private partnership initiatives to develop and share best practice.

11. Intelligence sharing

Contribute to public-private and cross-sectoral initiatives to address scams.

11.1 to 11.2 apply to:
Social Media Services
Social Media Services with Peer-to-Peer Marketplaces
Email Services
Messaging Services
Video Sharing Services
Paid Advertising Services on Digital Platforms

11.1. Work with the Government, the National Anti Scam Centre, the ACCC, the ACMA, law enforcement and other industry partners to:

11.1.1. Contribute to work undertaken by the NASC to coordinate action to combat scams.
11.1.2. Explore what data, both internal and external, could facilitate the identification and prevention of scams.
11.1.3. Share best practice and identify opportunities to share intelligence with other sector partners and other industries.

11.2. Signatories will respond to valid information requests from relevant regulators, under applicable legislation.

12. Communications

Provide information about scam risks and support counter-scam efforts.

12.1 to 12.3 apply to:
Social Media Services
Social Media Services with Peer-to-Peer Marketplaces
Email Services
Video Sharing Services
Paid Advertising Services on Digital Platforms
Messaging Services

12.1. Signatories commit to engaging with the National Anti Scam Centre and the ACCC, for example, to share information, guidance and learnings to combat scams.

12.2. Support efforts by the National Anti Scam Centre, the ACCC and/or consumer organisations' communications campaigns to help the public identify and avoid scams.

12.3. Continue engaging users with messaging regarding the risk they can face from scams such, for example, through in-product messaging, help pages or links to third-party resources.

13. Strategy & future proofing

Contribute to strategy development and future proofing exercises to stay ahead of the threat.

13.1 to 13.4 apply to:
Social Media Services
Social Media Services with Peer-to-Peer Marketplaces
Email Services
Video Sharing Services
Paid Advertising Services on Digital Platforms
Messaging Services

13.1. Develop an internal scams strategy that aims to see improvements in counter-scam efforts over time.

Note: DIGI strongly discourages any publication of these strategies which may provide perpetrators of scams with information to advantage their activity.

13.2. Analyse established and emerging methods and typologies of scams on Signatories’ relevant services.

13.3. Undertake cross-functional internal coordination to assess Signatories’ relevant services for the risks that future technologies pose, focusing on intervention points and opportunities to tackle scammers.

13.4. Share findings from Sections 13.2. with the National Anti Scam Centre and appropriate groups and organisations, where appropriate and permitted by law.

13.5. The code developer (DIGI) will review the code as needed in conjunction with Signatories, industry participants, Government, consumer bodies and other stakeholders as needed to ensure its continued relevance as a tool to effectively address scams in Australia. Any amendments to the Code will be published on the DIGI website.