effie Awards Australia

2026

# Case Study



**Entry ID Number**
1617

**Agencies**
BMF

**Client**
Department of Home Affairs / Australian Federal Government

**Title**
How Three Tiny Actions Made Australians Safer Online

**Category**
A09. Government

**Author**
Abigail Dawson
BMF

Advertising Council Australia | Marketing Association of Australia | Google

© This case study is the property of Advertising Council Australia (ACA) and protected by copyright and intellectual property laws throughout the world. The case study can be used for personal reasons only and should not be reproduced, distributed, sold or published without the express approval of ACA. Any educational facility interested in using the case history for educational purposes should contact effies@adcouncil.org.au

## Q1. EXECUTIVE SUMMARY & WHY DOES THIS CASE DESERVE AN AWARD?

Approximately every six minutes, an Australian falls victim to cybercrime[1](1). Despite years of rising threats and high-profile data breaches, Australians were settling into a dangerous complacency - cyber risk was highly salient but increasingly perceived as inevitable and largely beyond individual control. The proportion of Australians exhibiting high-risk cyber behaviours was growing, not shrinking. Awareness wasn't the problem… Action was.

Phase 4 of '**Act now. Stay Secure.'** set out to close the gap between knowing and doing. The strategy rested on a single insight: more information wouldn't break down apathy - but breaking down the actions, and making those feel emotionally consequential could. We set out to make doing nothing feel consequential, and reveal the solution as simple and within their power. Contrasting the enormity of the problem, with the simplicity of the action. A two-gear media approach scaled the emotional awareness narrative through TV, cinema and digital video, then intercepted Aussies in contextual moments - paused ads, nighttime targeting - to prompt specific action, with a singular message, when they were most achievable.

[redacted]

In a landscape where cyber threats cost the Australia economy an estimated $30 billion annually[4](4) and an average self-reported cost of cybercrime for individuals $33,000[5](5), even marginal behavioural improvement generates outsized economic returns. [redacted]

*SOURCES:*

*(1) ASD, Annual Cyber Threat Report 2024–25, Australian Signals Directorate*
*(2) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(3) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(4) CyberCX, 'Cyber crime costing the Australian economy $30 billion a year', 9 April 2025*
*(5) ASD, Annual Cyber Threat Report 2024-25, Australian Signals Directorate, November 2024 – average self-reported cost per individual cybercrime report*
*(6) Hall & Partners, ANSS Phase 4 Campaign Evaluation*




© 2026 Advertising Council Australia

## Q2. WHAT WAS THE STRATEGIC COMMUNICATIONS CHALLENGE?

### A cybercrime every six minutes, and a nation overwhelmed

Cybercrime refers to illegal activity directed at online devices and accounts. Common cybercrimes include identity theft, fraud, hacking, deliberate data breaches, ransomware and malware attacks that compromise devices, systems and personal data. It's one of the fastest-growing crime types in Australia. Unlike scams, which rely on deception and trickery, cybercrime often happens without the victim realising they've been exposed.

During the 2023-24 financial year, over 87,400 cybercrime reports were made to Australian law enforcement - on average that's one every six minutes[7](7). By the time the campaign concluded in March 2026, cyber crime costs had climbed YoY: individuals to $33,000 (+8%) and small businesses to $56,600 (+14%)[8](8).

The broader economic toll is staggering; with an estimated impact to Australia's economy at $29-30 billion annually[9](9) With Optus, Medibank and Latitude collectively exposing over 30million records in 2022-23 alone[10](10), the threat wasn't theoretical. It was personal, but people felt powerless.



### Knowing more, but not doing more

The campaign supports the delivery of the Australian Government's *2023–30 Australian Cyber Security Strategy*. Phase 3 of '**Act Now. Stay Secure.'** had done what it set out to do - raise awareness of three protective behaviours: use a unique and strong passphrase on every account, install all software updates to keep devices secure, and always initiate multi-factor authentication (MFA). But awareness wasn't translating into consistent action.

[redacted] *Vulnerability is measured based on stated security behaviours and attitudes. Those most vulnerable Australians were disproportionately younger and male, more likely to identify as First Nations, live with a disability or be culturally diverse Australians.)* Phase 4 had to close the gap between knowing and doing - converting passive awareness into consistent, habitual action among the Australians most at risk.


© 2026 Advertising Council Australia



**A nation locking the front door, but keeping their digital world wide open**

The research uncovered a perverse dynamic. As banks, telcos and government services increasingly mandated security measures like MFA and strong passwords, people developed a false sense of security. They applied rigorous protections to these 'high-stakes' interactions but cut corners elsewhere - social media, streaming, online shopping, public Wi-Fi[12](12).

*"When the companies force us to use two-factor checking it feels like it's not as much my responsibility anymore."*

This created a behavioural hierarchy - a two-tier system of 'compulsory' and 'discretionary' cyber security - that left people exposed precisely where they felt safest.




© 2026 Advertising Council Australia

**The sense of inevitability was breeding apathy**

[redacted]

[redacted]



**Perceived security ≠ less responsibility - the cycle we had to break**

We faced a campaign paradox. Every new layer of platform security - and business-mandated protection - was quietly eroding people's sense of personal responsibility[16](16). Individual cyber security behaviors protect the gaps that businesses can't fully control; software updates patch vulnerabilities on personal devices, strong passphrases reduce the impact of credential theft, and MFA adds a second layer of protection if passwords are compromised. The challenge: every high-profile breach reinforced the belief that individual effort was futile.

We needed to break through complacency, dismantle the false hierarchy between 'mandatory' and 'individual' security, and convert passive knowledge into active, habitual behaviour.

*SOURCES:*


*(7) ASD, Annual Cyber Threat Report 2023–24, Australian Signals Directorate*
*(8) ASD, Annual Cyber Threat Report 2024–25, – average cost per cybercrime report for small business*
*(9) CyberCX, 'Cyber crime costing the Australian economy $30 billion a year', 9 April 2025.*
*(10) OAIC, Notifiable Data Breaches Reports 2022–23; public reporting on Optus, Medibank, Latitude breaches*
*(11) Verian, ANSS Phase 4 Developmental Research Report, p.16 – vulnerability index comparison*
*(12) Verian, ANSS Phase 4 Developmental Research Report, p.12 – behavioural hierarchies and context-driven risk perception*
*(13) Verian, ANSS Phase 4 Developmental Research Report, p.19 – high vulnerability group attitudes*
*(14) Verian, ANSS Phase 4 Developmental Research Report, pp.22–27 – segmentation of high vulnerability group*
*(15) Verian, ANSS Phase 4 Developmental Research Report, p.20 – information seeking behaviour, high vulnerability group*
*(16) Verian, ANSS Phase 4 Developmental Research Report, p.13 – shifting perceptions of government's role*



© 2026 Advertising Council Australia

## Q3. WHAT WERE YOUR OBJECTIVES? State specific goals.

Federal government campaigns are evaluated using a pre-campaign benchmark for topic awareness, understanding and relevant attitudes and behaviours, then track these during the course of the campaign. Shifts from benchmark determine strength of impact.

The campaign was to support delivery of the Australian Government's 2023-30 Cyber Security Strategy in efforts to become one of the world's most secure nations. The full impact of the campaign will have cumulative effects, but there were specific success criteria for this phase:

**PRIMARY TASK: Empower Australians to take control of their cyber security by demonstrating why it's important and what they must do.**
[redacted] the proportion exhibiting high-risk behaviours had grown. Awareness wasn't the problem. A culture of avoidance, apathy and false confidence was.

We needed to make cyber security feel personal and actionable - connecting the emotional weight of what's at stake to the simple small steps you can take.

**OBJECTIVE 1: Build campaign recognition, increase understanding of cyber threats and drive emotional engagement that compels action**

- Campaign recognition above [redacted] whole-of-government norm [redacted]
- Prompted message takeout above [redacted] government norm
- 'Easy to understand' above [redacted] government norm
- 'Believable' above [redacted] government norm
- NET involvement (i.e. feeling compelled to act) above [redacted] government norm

**OBJECTIVE 2: Reduce the proportion of Australians in the high vulnerability group**

- Measurable reduction from [redacted] high vulnerability benchmark

**SECONDARY TASK: Drive uptake of key cyber safe behaviours by educating Australians on how simple, individual actions applied consistently, can have a significant impact on their cyber security.**
Consistency was a key barrier to strengthening cyber protection. We needed to move more Aussies beyond passive awareness into habitual, consistent action.

**OBJECTIVE 3: Increase action across key cyber safe behaviours**

- NET campaign-related action during the campaign period above [redacted] benchmark
- Increase in people who:
  - always set up MFA when available
  - install software updates
  - use unique and strong passphrases

**OBJECTIVE 4: Build understanding of the importance of consistent action**

- Increased agreement that:
  - 'simple, individual actions can have a significant impact on my personal cyber security' from [redacted] benchmark
  - 'I understand the importance of consistently engaging in cyber secure behaviours' from [redacted] benchmark

**TERTIARY TASK: Build recognition of the Australian Government as the trusted voice and authority on cyber security.**
Research showed the Government's perceived role was shifting towards regulation. We needed to maintain relevance as an educational voice amidst this shift[17](17), positioning the Government not as sole protector, but as a credible educator and partner in shared cyber security responsibility.

**OBJECTIVE 5: Increase positive perception of the government as a trusted source and voice**

- Increase perceptions of "The Aus Gov is a trusted authority for information on how to be cyber secure"
- Increase perceptions of "The Australian Government is a trusted voice trusted voice when it comes to cyber security"

*SOURCES:*

- *All Baselines from Hall & Partners, ANSS Phase 4 Campaign Evaluation*

*(17) Verian, ANSS Phase 4 Developmental Research Report p.13*


© 2026 Advertising Council Australia

## Q4. WHAT WAS YOUR STRATEGY AND HOW DID YOU GET THERE?

### The threat was evolving, but messaging wasn't keeping pace

Phase 4 was an evolution of Phase 3, so the core strategy remained. Home Affairs had previously run "Beat Cybercrime in your Downtime" - a deliberately light-hearted campaign that demonstrated easy, quick actions for everyday Australians. Proving the risk, no matter who or where you are. But by 2023, several corporate breaches exposed millions of Australians' data. Given the tension between the seriousness of cyber crime, and the light-hearted tone of the existing campaign, we needed to start fresh.

[redacted]

[redacted]

### More advice and information isn't the solve for apathy

Behavioural research confirmed what we were seeing: simply providing information on the threat - however clear, engaging or urgent - wasn't enough to shift behaviour.[redacted] The challenge was motivation, not knowledge. And the barrier to motivation was a deeply held belief that individual action was futile against the scale of the threat. We needed to break this apathy - not with more information, but with emotion.

### The unlock: contrast the enormity of consequence with the simplicity of prevention

Rational argument wasn't cutting through, we needed to make people *feel* the weight of not acting. But scaring our audience into action would only reinforce the already felt helplessness.

The unlock was in the *contrast*. Dramatising the significant consequence that cascades from a single moment of inaction. That gap - between the scale of the impact and the ease of the fix - is where motivation thrives.

Our messaging approach for Phase 4 reinforced this strategy. Rather than highlighting threats broadly, we broke down the actions to make them feel small, everyday and immediate. Not a checklist, but three micro-actions anyone could take in minutes, shared in sequence so as to not overwhelm the audience. This turned the perceived threat of scale on its head: *the threat feels enormous, but the defence is tiny.*

**STRATEGY**

**GET** Australians who feel helpless and have stopped believing their actions make a difference

**TO** Reclaim control by consistently taking three simple cyber security actions

**BY** Dramatising the cascading impacts of inaction to make doing nothing feel consequential, and reveal the solution as simple and within their power.

**CORE THOUGHT: EVERY LITTLE THING WE DO TO PROTECT OURSELVES CAN MAKE A BIG DIFFERENCE.**

[17] *Verian, ANSS Phase 4 Developmental Research Report p.13*
[18] *Verian, ANSS Phase 4 Developmental Research Report p.24*
[19] *Behavioural Economics Team of the Australian Government (BETA), 'Password123' report*


© 2026 Advertising Council Australia

## Q5. HOW WAS YOUR STRATEGY BROUGHT TO LIFE?

### The power of showing, not shouting

The strategy demanded a creative device that could hold two extremes in a single narrative - the enormity of what you could lose, and the simplicity of what could have saved it.

Each film drops us into someone's life mid-freefall. We watch the dominoes fall - financial chaos, emotional toll, identity fear - cascading in ways that feel real and relatable. Then, the film rewinds through the wreckage, back past every consequence, to land on the single, mundane moment that started it all: a multi-factor authentication (MFA) prompt dismissed, a software update snoozed, a weak password reused. The gut-punch lands in the tension - *all of that, preventable by this?*

### Filmic device to exaggerate the strategy

The rewind device made the strategic contrast visceral. The audience feels the full weight of the consequence before they see how small the preventative action is. The juxtaposition helps shift motivation from abstract to personal. Combatting overwhelm with agency.

### Serious without scaring, empowering without lecturing

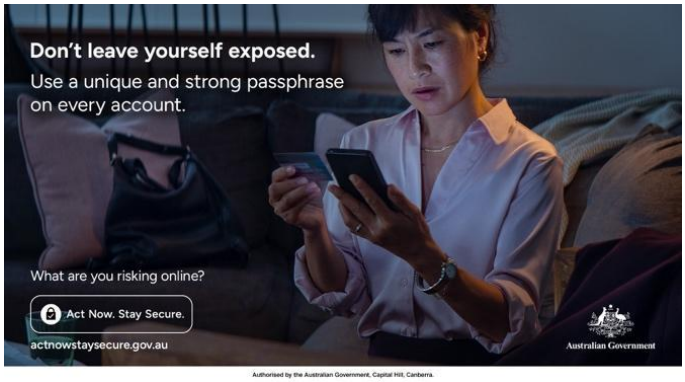
[redacted]The creative used inclusive language of 'we' and 'our', positioning the government as doing its part while empowering individuals to build on this. '**Act Now. Stay Secure.'** conveyed both urgency and agency - not blame. It was important we used relatable talent that resonated for all Australians, and simple messaging that translated effectively across multiple languages.

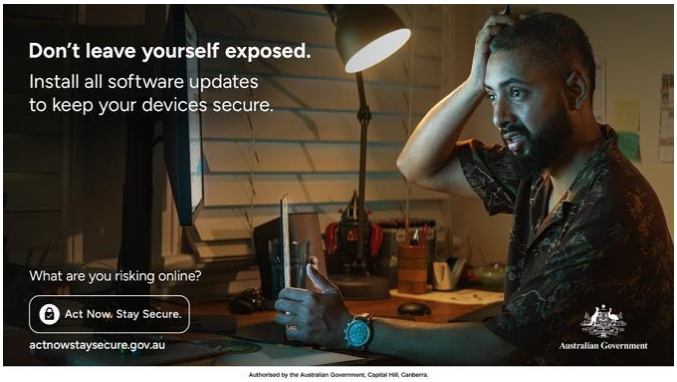
### Micro-actions, not a check-list

To make the solution feel manageable, each execution resolved on one of three behaviours:

- **Use a unique and strong passphrase on every account**
- **Install all software updates to keep devices secure**
- **Always set up MFA**

Deliberately small, and targeting moments to communicate more tactfully. Not presented as a comprehensive cyber security programme - they were positioned as the tiny actions that stand between you and the avalanche you just witnessed. The emotional narrative carried the weight; the actions served as the almost-too-easy resolution.




### Prioritising what puts people most at risk

Messaging was prioritised based on where individuals were most exposed, and where they had the most control to reduce that exposure. Software updates and passphrases - actions within personal control - elevated as the highest-impact behaviours.

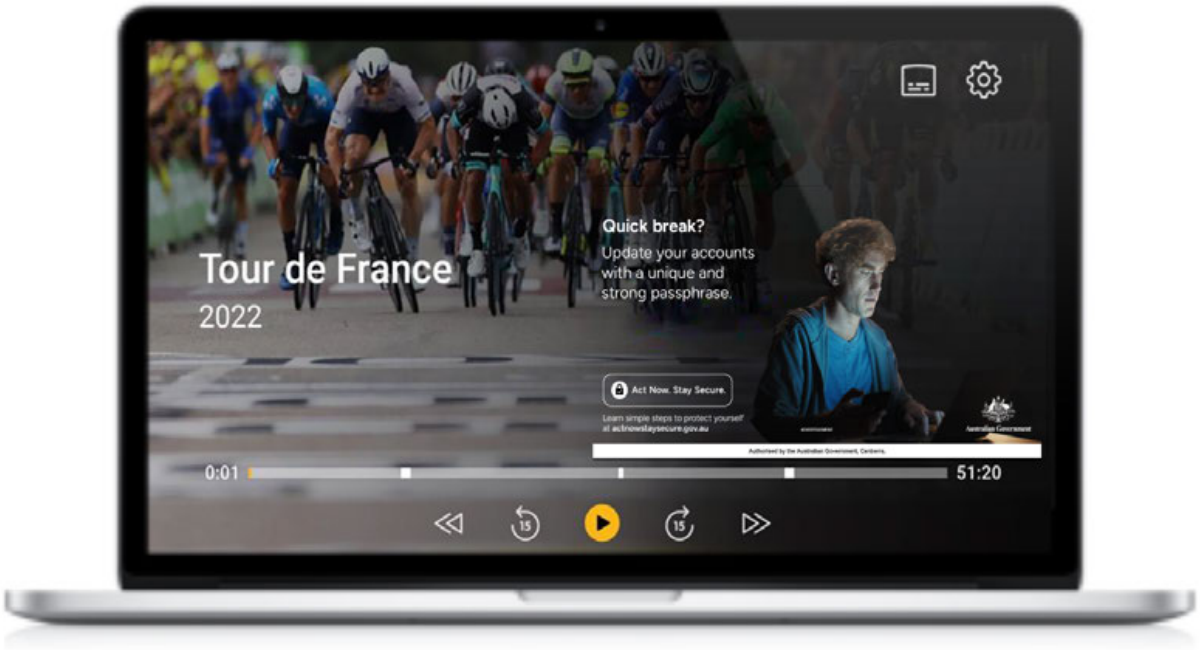
MFA, increasingly mandated by banks and platforms, was reframed as reinforcement, to be implemented across your whole digital life. Spend was concentrated where messaging could actively reduce risk and motivate new behaviours.


© 2026 Advertising Council Australia

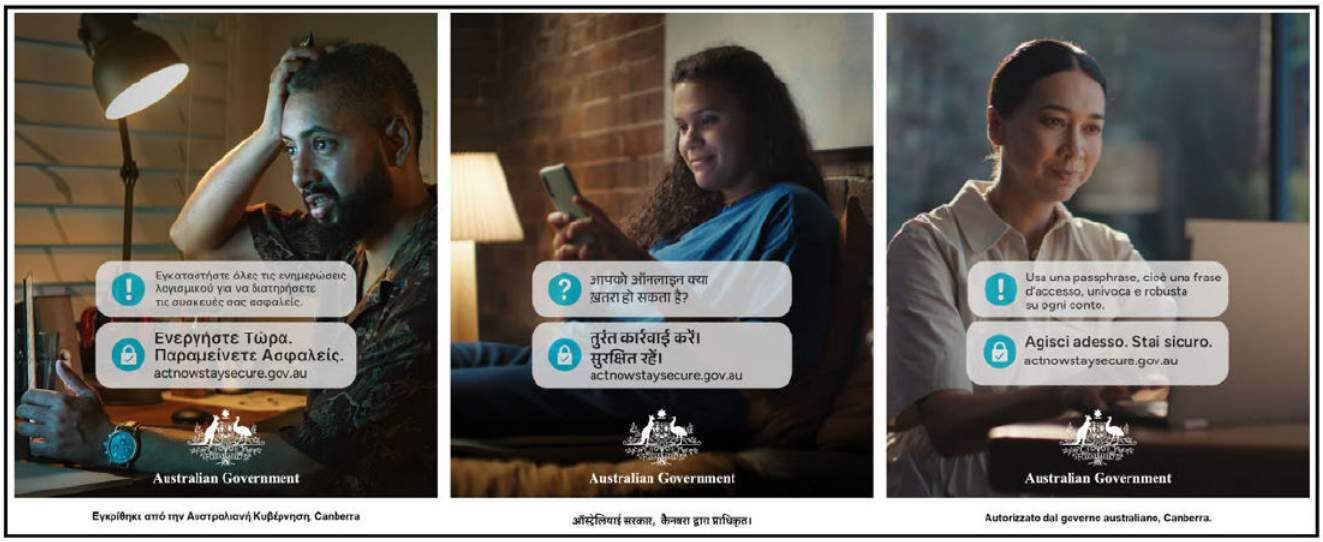
**Turning idle moment into action**

The media strategy was designed to intercept exposure in real time. TV, cinema and digital video was leveraged to scale the consequences of inaction - making the risk visible, tangible and immediate. High-impact-pause, audio and social targeted contextual moments where cyberthreat was relevant, but likely not top of mind.

SVOD and BVOD pause ads appeared following a pause from watching content - reframing idle time as a window of vulnerability, and an opportunity to update[21](21). Night-time social and digital targeted the hours devices sat inactive - prompting updates before risk could accumulate. Gaming loading screens captured users mid-delay. Scroll-stopping dominations across X and Reddit disrupted passive browsing with direct passphrase prompts.




For CALD audiences, assets were placed on culturally-specific platforms including WeChat and RedNote alongside mainstream channels, with Auslan-translated tutorials extending accessibility further.




**Source: https://www.actnowstaysecure.gov.au Translated Asset Resource Hub**

*SOURCES:*

*(20) Kantar Public, Sprint 1 Strategic Recommendations, September 2023*

*(21) UM, ANSS Phase 4 Media Performance Report*


© 2026 Advertising Council Australia

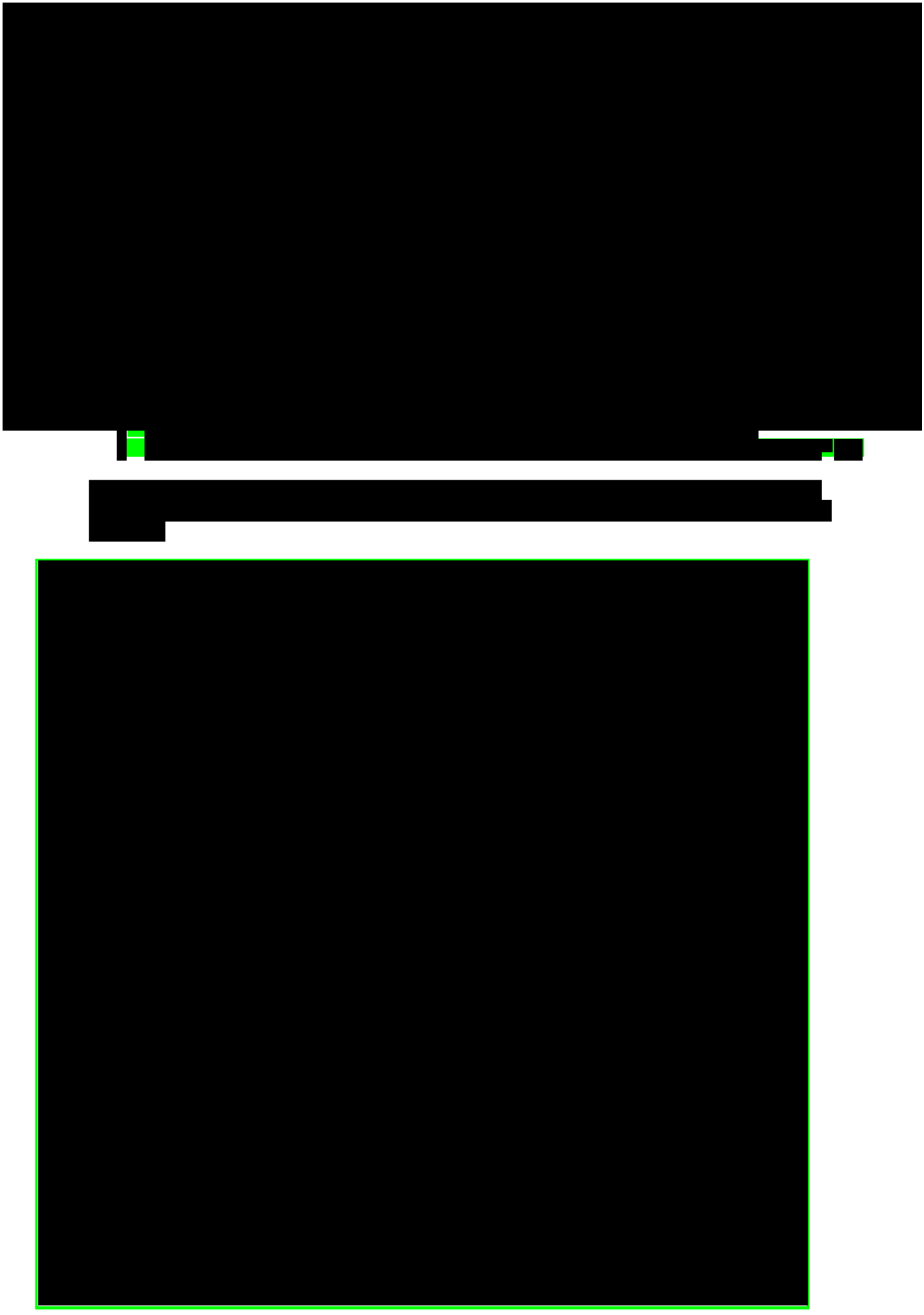
## Q6. HOW DO YOU KNOW THAT YOUR CAMPAIGN WAS SUCCESSFUL?

Results exceeded expectations.






© 2026 Advertising Council Australia




© 2026 Advertising Council Australia



*SOURCES:*


*(22) Hall & Partners, ANSS Phase 4 Campaign Evaluation, Village Debrief 1, April 2026*
*(23) Hall & Partners, ANSS Phase 4 Campaign Evaluation — campaign recognition*
*(24) Hall & Partners, ANSS Phase 4 Campaign Evaluation — core on-strategy message takeout*
*(25) Hall & Partners, ANSS Phase 4 Campaign Evaluation — advertising diagnostics vs norms*
*(26) Hall & Partners, ANSS Phase 4 Campaign Evaluation — advertising diagnostics vs norms*
*(27) Hall & Partners, ANSS Phase 4 Campaign Evaluation — NET Involve 75% vs 49% norm*
*(28) Hall & Partners, ANSS Phase 4 Campaign Evaluation — vulnerability index*
*(29) Verian, ANSS Phase 4 Developmental Research Report, 14 January 2025, p.16*
*(30) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(31) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(32) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(33) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(34) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(35) Hall & Partners, ANSS Phase 4 Campaign Evaluation*
*(36) Department of Home Affairs, Website Analytics, March 2026*



© 2026 Advertising Council Australia

## Q7. WAS THE CAMPAIGN A GOOD INVESTMENT?

[redacted]



[redacted]

[redacted] *Annual Cyber Threat Report 2024–25, October 2025*

[redacted]

[36] *Department of Home Affairs, Website Analytics, March 2026*

[37] *Australian Institute of Criminology - Cybercrime in Australia 2024 p.6*

[redacted] *Verian, ANSS Phase 4 Developmental Research Report, 14 January 2025, p.19*


© 2026 Advertising Council Australia

## Q8. DEMONSTRATE THAT THE RESULT WAS NOT DUE TO OTHER FACTORS

**Are results driven by the cultural climate of data breaches?**

High-profile breaches amplified awareness - but were working against behaviour. [redacted]

**Couldn't the rise in mandated corporate security measures account for the behavioural shift?**

Banks, telcos and government services increasingly mandated MFA and stronger passwords over this period. But this was reinforcing inaction and apathy creating a false sense of security that reduced personal responsibility[46](46). Mandated measures were making people *less* careful in other areas of their online life. Our messaging specifically countered this - 'every account', 'all software updates', 'always' - to break the assumption that what businesses enforce is enough.

**Couldn't it just be the weight of media spend?**

[redacted] But results weren't a function of spend. The campaign outperformed government norms across virtually every metric - many representing campaigns with comparable or larger budgets[47](47) The approach to contextual media (pause ads, nighttime targeting, gaming platforms) was specifically identified as contributing to enhanced recognition and cut-through, over and above what awareness activity alone could deliver[48](48).

*SOURCES:*

*(44) ANSS Phase 4 Developmental Research Report, p.10*
*(45)ANSS Phase 4 Developmental Research Report, p.16 - vulnerability index increase*
*(46)ANSS Phase 4 Developmental Research Report, p.12*
*(47)Hall & Partners, ANSS Phase 4 Campaign Full Evaluation Report, 2026*
*(48) UM, ANSS Phase 4 Media Performance Report, p.3; Hall & Partners, ANSS Phase 4 Campaign Full Evaluation Report, 2026*

## Q9. GIVE CONTEXT TO BUDGET IN COMPARISON TO COMPETITORS.

## Q10. GIVE CONTEXT TO THE BRAND'S OVERALL BUDGET.

**Not Applicable**

## Q11. MEDIA BUDGET ELABORATION

Budget was heavily weighted to paid media. High awareness, high impact channels were leveraged to elicit an emotional connection - turning video-watching minutes into cyber security education. Followed by contextual, high-impact placements - pause ads, nighttime targeting, gaming integrations - to prompt specific actions in moments where the behaviour was most relevant and achievable. CALD-specific media received dedicated investment given overlap between these diverse communities and the high-vulnerability target audience. Investment was comparable with other Australian Government campaigns required to effectively reach all Australian adults.

## Q12. DESCRIBE OWNED MEDIA ACTIVITY

Owned media channels included a landing page for actnowstaysecure.gov.au housing resources, real stories from Australians who experienced cyber crime, and a list of cyber safe actions to employ.


© 2026 Advertising Council Australia

## Q13. OUTLINE ANY SPONSORSHIPS

N/A

## Q14. OUTLINE COMMUNICATION TOUCHPOINTS

- Television
- Cinema
- Digital video
- Social media
- Digital audio & podcasts
- OOH
- Regional & CALD Press
- PR including community outreach, case studies, influencer, broadcast coverage
- Search
- Website


© 2026 Advertising Council Australia