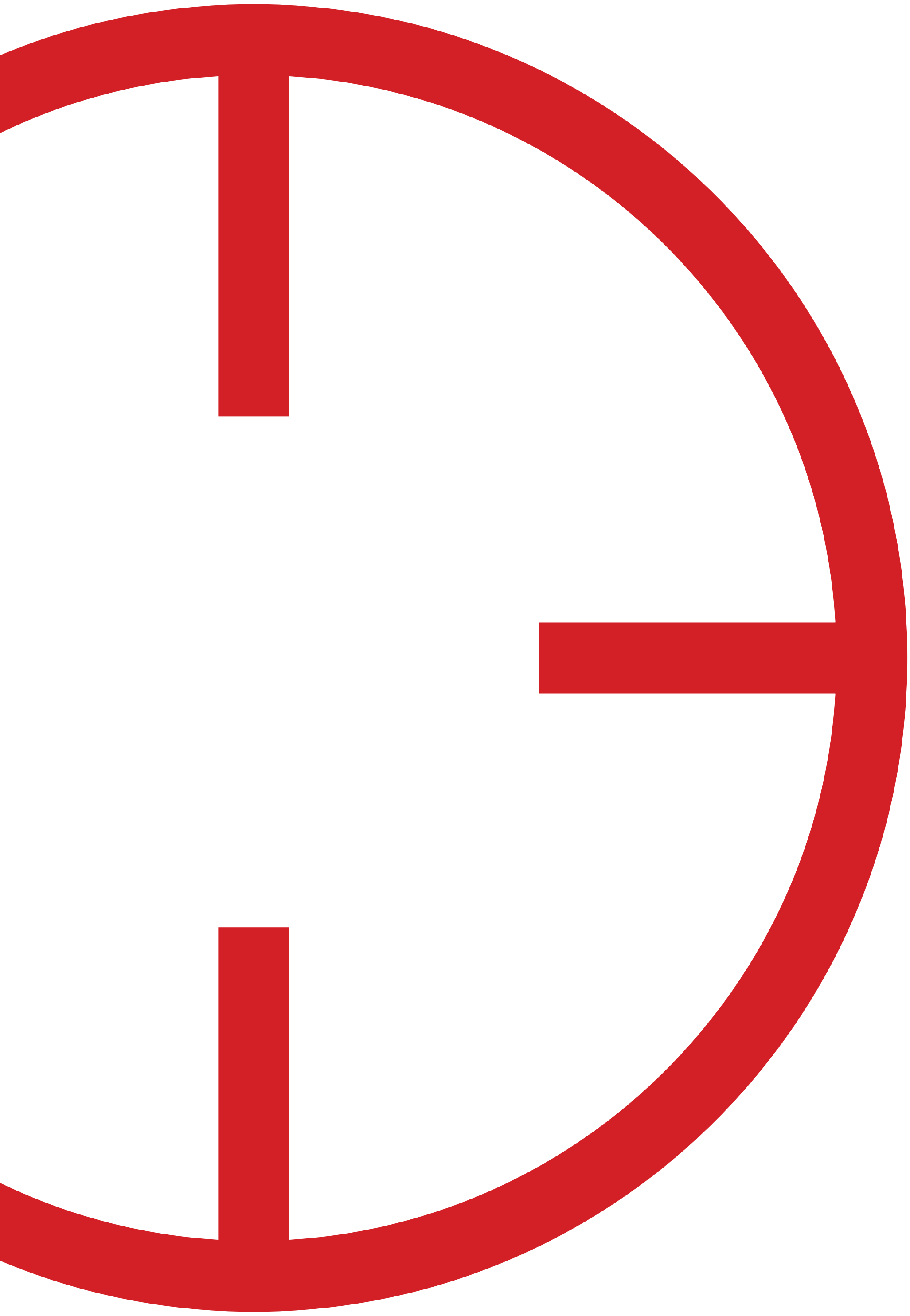
Scams & Identity Theft



CAMPAIGN PROPOSAL

SCAMERA SCAMWATCH

Contents

Executive Summary

In an age where humans are becoming increasingly reliant on technology and have the habit of sharing personal information online, the number of scams that are delivered to people's devices increases by the year. Scams are evolving, and they can take any form. Reporting scams can help people feel at ease and reporting can help prevent them from reaching more people.

This document proposes a campaign strategy that is centred on highlighting the danger of scam alerts delivered on digital devices. The campaign urges individuals to identify, capture and report scam notifications in a safe fashion. It will communicate the message through digital media formats such as a mobile application, website, social media posts as well as traditional print media such as posters and bus-stop banners.

The Challenge

- The Issue
- The Brief
- The Sponsor

The Issue

Identity theft is a growing issue due to the rapid growth of the internet and the increasing dependence on e-commerce, and social media has created an opportunity for cyber criminals to steal and utilise personal information to exploit people's identity. According to Privacy Australia (Ellis 2023), identity theft occurs when "a criminal appropriates an individual's personal information such as name, address, date of birth or Social Security number to assume that person's identity to commit theft or multiple types of fraud." Fraud in this case is generally the theft of money from vulnerable individuals, and it is appealing method to criminals as its relatively risk-free and due to the ease of concealment (Ellis 2023). Due to the deceptive nature of scams and fraud, people may not always be aware that they have been exposed to or responded to a scam.

The most common types of scams are phishing, financial advice, buying or selling, computer support, business email compromise (BEC) and ransomware.

A person would be considered exposed if a person received an unsolicited request, invitation, offer or notification and read, reviewed, or listened to the material. Being exposed to a scam does not constitute being a victim of scam. If a person, after being exposed to a scam, sought further information or provided personal or financial information or accessed links associated with the scam, then they are victims of a scam.

300,000

cyber-crimes are committed every year in Australia alone.

Every 7 minutes

a cybercrime is reported to the Australian Cyber Security Centre (ACSC).

1 in 10

URLs are malicous that contain ransomware.

23% to 47%

is the statistic that describes scam text exposures in the last two years, which has doubled since 2020.

9.5 Million people were affected.

The Brief

Campaign Goal

To create a campaign that targets young Australian adults and urges them to take precautionary measures regarding scam texts and emails that are are involuntary delivered to the user's device. The purpose of the campaign is to shed light into the advanced, new era of scams, and prevent cyber-crimes such as identity theft by prompting users to identify and report scams. With information spread from the youth to older generations, the campaign will hopefully inspire the wider community to take action against scammers in a safe way without engaging with or interacting with scammers themselves.

The Context

The target market of the campaign will be targeted towards young Australian adults aged between 18 to 28. The campaign will communicate to both males and females who own devices such as phones, laptops and tablets and who regularly use social media by posting and uploading content. The campaign will also warn the older generation that are aged between 45-65 who are in a more vulnerable position of being a scam victim. The younger target market who tend to be more progressive for change will be able to spread the word and help the older generation (such as family members).

Brand Proposition

The campaign will shed light into the evolving scam age, where scammers will find alternative ways to commit cyber crimes (such as humour or pretending to be a family member.). The tone of the campaign will be informative, serious, ominous to urge the audience to take quick action. Individuals may not feel powerful having to deal with a potential scam, and therefore the messaging will be bold, confident, and clearly instruct the viewer what to do and what steps to take.

Key Insights

In Australia, cyberattacks have become more prevalant, smart and cunning in a world where Artificial Intelligence is taking over. The future of technology seems amazing with it's advancements but with that, it means that technology is also very unpredictable and that can be daunting. Billions of dollars every year are spent trying to prevent hackers and data breaches, and so protection of personal data and internet use must be taken seriously. In Australia alone, 300,000 cyber-crimes are committed every year and in 2022, a cybercrime was reported to the ACSC (Australian Cyber Security Centre) every 7 minutes. There are many people who don't know they've been scammed or have been exposed to one, so imagine the scams that are not reported. People are most commonly exposed to scams via text (47%) or over the phone (48%), and exposure via text has doubled from 23% to 47% from 2020 to 2022. The future of scams and for scam victims only seems more grim when these statistics are observed.

The Media

As the target audience are users of social media, the campaign will be implemented on social media platforms like Instagram where posts can be easily shared to a larger community using hashtags. With regards to OOH advertising, the campaign will be advertised as posters and banners on bus stops and as transit ads in populated areas such as the central business district in order to effectively reach a wider audience (both primary and secondary audiences). Ultimately, the campaign will entice viewers to scan and download an application dedicated for scam reporting.

The Sponsor

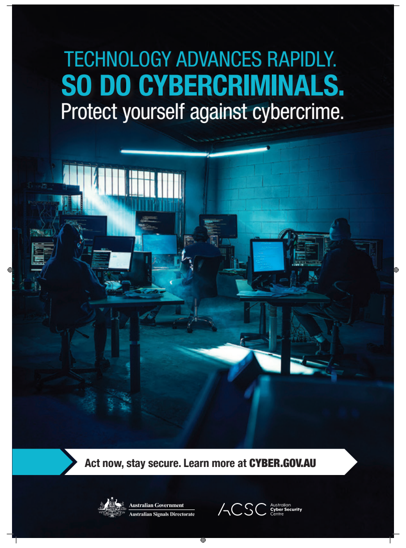
SCAMWATCH

The sponsor of the campaign is Scamwatch, a division of the Australian Competition and Consumer Commission (ACCC) entirely dedicated to assist victims of scams. Scamwatch is where Australians are advised to report scams to, as they use these reports to identify new scams, disrupt them and warn consumers about smart, new scams. They provide news and alerts for scam related information and statistics on their main homepage. They urge individuals to sign up to their email newsletter to be alerted via their 'scamwatch radar'.

The Context

- Benchmarking
- Positioning
- Audience Research
- Personas

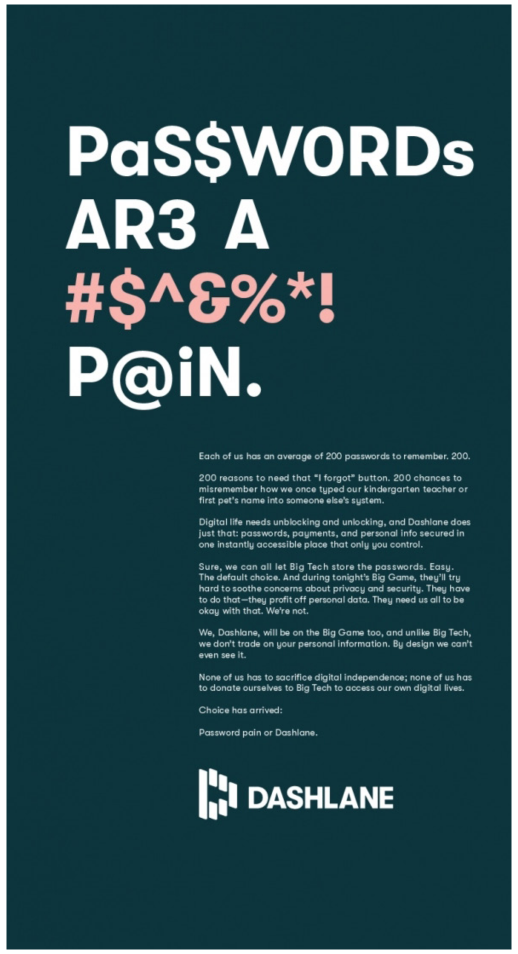
Benchmarking


TECHNOLOGY ADVANCES RAPIDLY.
SO DO CYBERCRIMINALS.
Protect yourself against cybercrime.
Act now, stay secure. Learn more at CYBER.GOV.AU
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

PROTECT YOURSELF
AGAINST CYBERCRIME
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

Act Now, Stay Secure (2021)

This campaign was developed to highlight the importance of updating devices and software to help prevent cybercriminals from taking advantage of personal, private data stored online. It educates and informs Australians about cyber threats and promotes cyber.gov.au as the leading cybersecurity resource, sharing and promoting easy-to-follow cybersecurity advice for individuals, businesses and organisations alike. The main aims of the campaign are to educate & spread awareness. The high tech aesthetic and visuals that utilise blue reflect the sophistication of advanced technologies and screens, which is relevant to the overarching theme of digital technology.



PaS$WORDs
AR3 A
#$^&%*!
P@iN.

Each of us has an average of 200 passwords to remember. 200.

200 reasons to need that "I forgot" button. 200 chances to misremember how we once typed our kindergarten teacher or first pet's name into someone else's system.

Digital life needs unblocking and unlocking, and Dashlane does just that: passwords, payments, and personal info secured in one instantly accessible place that only you control.

Sure, we can all let Big Tech store the passwords. Easy. The default choice. And during tonight's Big Game, they'll try hard to soothe concerns about privacy and security. They have to do that—they profit off personal data. They need us all to be okay with that. We're not.

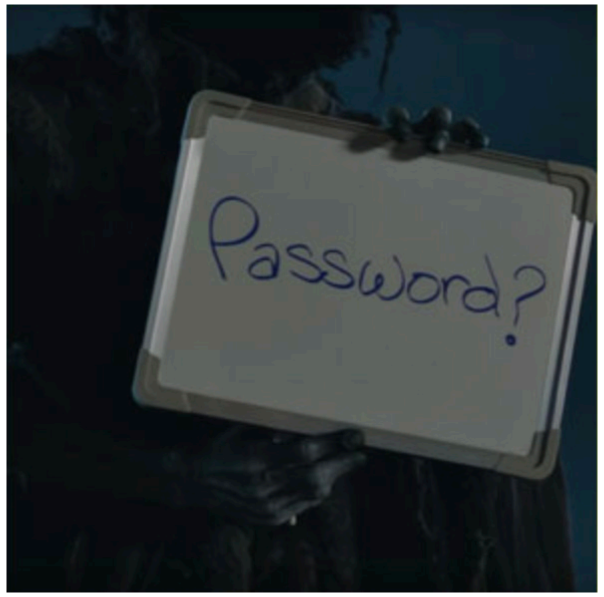
We, Dashlane, will be on the Big Game too, and unlike Big Tech, we don't trade on your personal information. By design we can't even see it.

None of us has to sacrifice digital independence; none of us has to donate ourselves to Big Tech to access our own digital lives.

Choice has arrived:

Password pain or Dashlane.

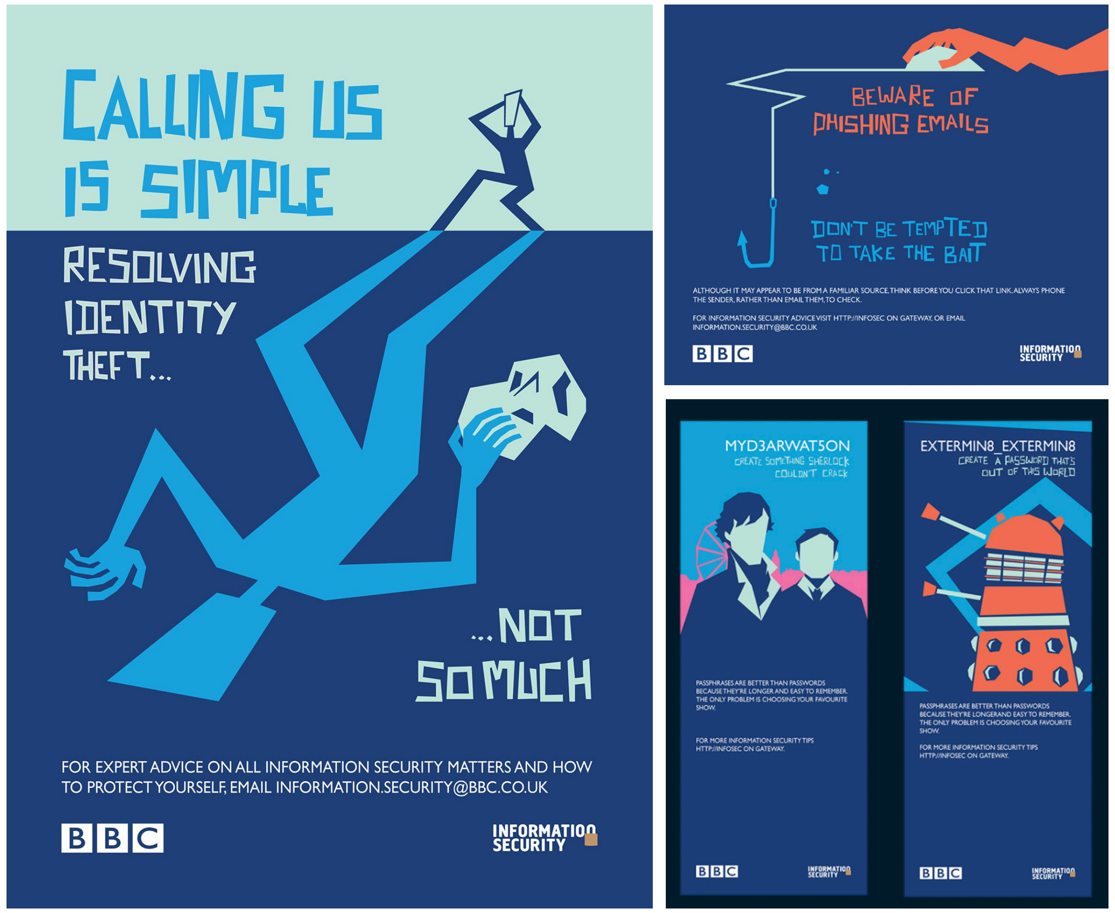
DASHLANE



Password Pain or Dashlane (2020)

Dashlane is a password security manager, and this campaign urges viewers to create safe passwords with the help of their service. In their campaign video advertisment, a situation is shown to be very grim and dark if one is made to enter a password they do not remember. It then shows a paradise that they can enter if they remeber their password. It uses humour and satire to reminds viewers of the frustration of not recalling passwords and not using a password manager service. The catchphrase 'Password Pain' is memorable, relatable and unique, making their brand approachable and their call-to-action of picking either password pain or their service, very enticing.

Benchmarking


CALLING US IS SIMPLE
RESOLVING IDENTITY THEFT...
...NOT SO MUCH
BBC
INFORMATION SECURITY
BEWARE OF PHISHING EMAILS
DON'T BE TEMPTED TO TAKE THE BAIT
MYD3ARWAT5ON
CREATE SOMETHING SHERLOCK COULDN'T CRACK
EXTERMIN8_EXTERMIN8
CREATE A PASSWORD THAT'S OUT OF THIS WORLD

FOR EXPERT ADVICE ON ALL INFORMATION SECURITY MATTERS AND HOW TO PROTECT YOURSELF, EMAIL INFORMATION.SECURITY@BBC.CO.UK

ALTHOUGH IT MAY APPEAR TO BE FROM A FAMILIAR SOURCE, THINK BEFORE YOU CLICK THAT LINK. ALWAYS PHONE THE SENDER, RATHER THAN EMAIL THEM, TO CHECK.

FOR INFORMATION SECURITY ADVICE VISIT HTTP://INFOSEC ON GATEWAY, OR EMAIL INFORMATION.SECURITY@BBC.CO.UK

PASSPHRASES ARE BETTER THAN PASSWORDS BECAUSE THEY'RE LONGER AND EASY TO REMEMBER. THE ONLY PROBLEM IS CHOOSING YOUR FAVOURITE SHOW.

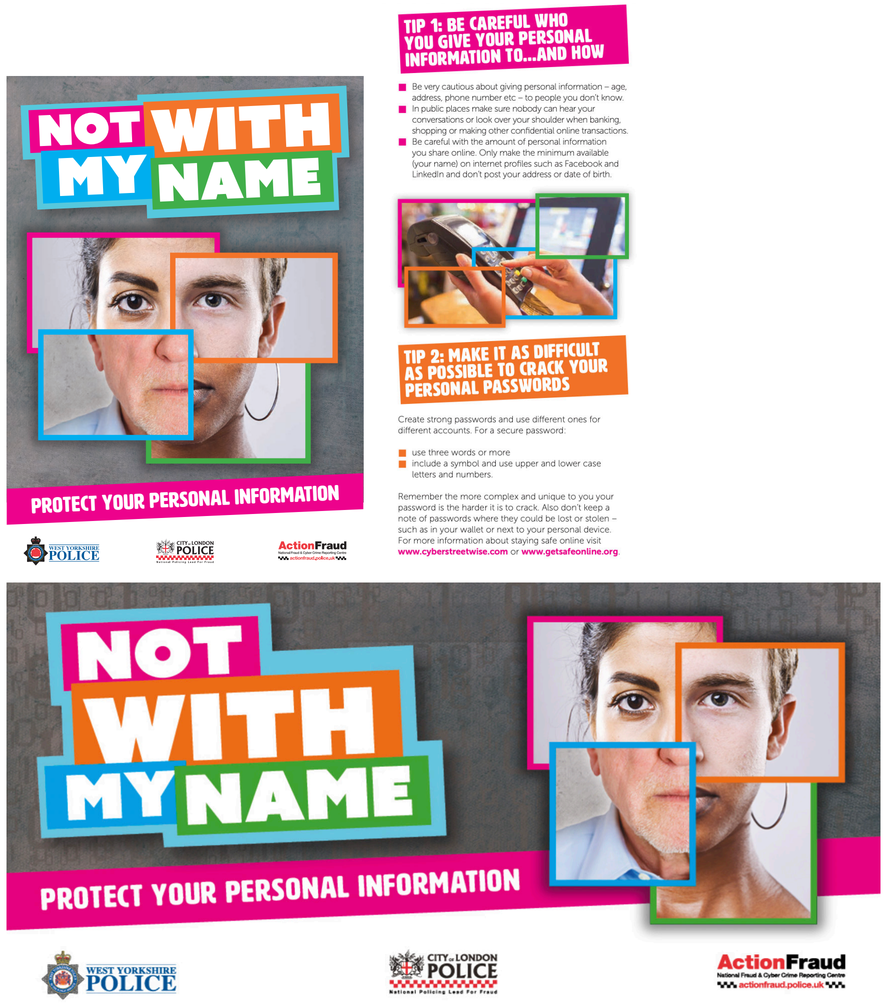
FOR MORE INFORMATION SECURITY TIPS HTTP://INFOSEC ON GATEWAY.

PASSPHRASES ARE BETTER THAN PASSWORDS BECAUSE THEY'RE LONGERAND EASY TO REMEMBER. THE ONLY PROBLEM IS CHOOSING YOUR FAVOURITE SHOW.

FOR MORE INFORMATION SECURITY TIPS HTTP://INFOSEC ON GATEWAY.

Information Security Threats (2014)

This is a series of posters and illustrations commisioned by BBC. This project was created to raise awareness on a number of technological threats such as identity theft and phishing. It uses geometric illustrative graphics that contrast to draw attention and have a memorable impact on the viewer. It works to encourage viewers to think about the current protection systems they might have or don't have in place, and urges them to take further steps to protect their information. It uses play on words in their copywrighting and references pop-culture to engage viewers and delivers their message quickly and simply. It also compares two situations, being a victim and not being a victim, to shed light into scams and identity theft.


NOT WITH MY NAME
PROTECT YOUR PERSONAL INFORMATION
WEST YORKSHIRE POLICE
CITY OF LONDON POLICE
ActionFraud

TIP 1: BE CAREFUL WHO YOU GIVE YOUR PERSONAL INFORMATION TO...AND HOW

- Be very cautious about giving personal information – age, address, phone number etc – to people you don't know.
- In public places make sure nobody can hear your conversations or look over your shoulder when banking, shopping or making other confidential online transactions.
- Be careful with the amount of personal information you share online. Only make the minimum available (your name) on internet profiles such as Facebook and LinkedIn and don't post your address or date of birth.

TIP 2: MAKE IT AS DIFFICULT AS POSSIBLE TO CRACK YOUR PERSONAL PASSWORDS

Create strong passwords and use different ones for different accounts. For a secure password:

- use three words or more
- include a symbol and use upper and lower case letters and numbers.

Remember the more complex and unique to you your password is the harder it is to crack. Also don't keep a note of passwords where they could be lost or stolen – such as in your wallet or next to your personal device. For more information about staying safe online visit www.cyberstreetwise.com or www.getsafeonline.org.

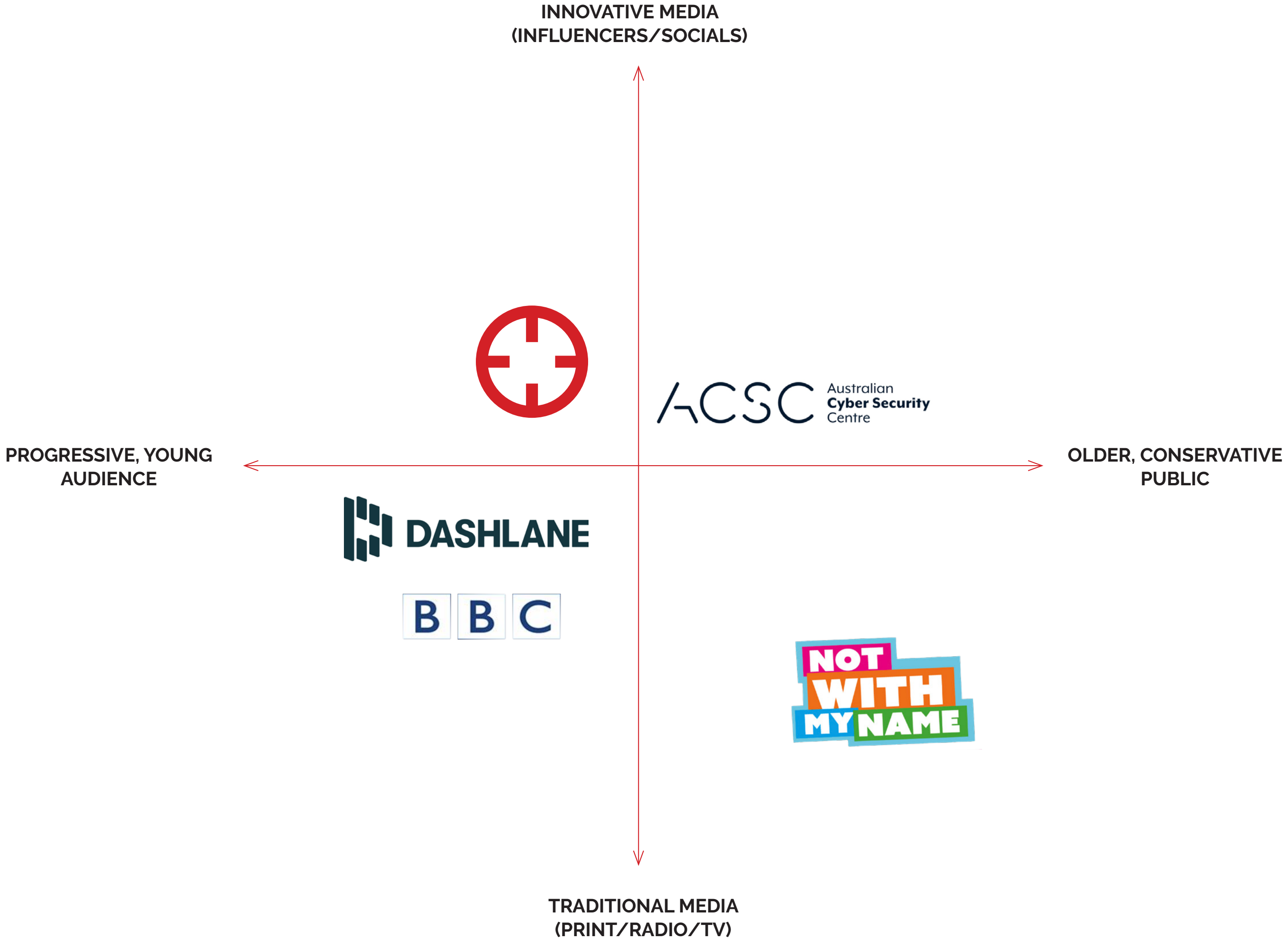
Not With My Name (2016)

The 'Not with my Name' campaign was created by part of the West Yorkshire Police Department, with the aim to target criminals and combat the rising threat that greatly impacts people's lives and society at large. It is constructed in a leaflet format, with the purpose to be distributed to people to educate, inform and spread awareness. It highlights alarming statistics, shares insights and provides advice and tips on how to protect personal information. It also uses bright, intense colours and graphics to gain attention. The graphics and text are bold to emphasize the unforgiving and fierce perspective of the viewer and potential victim.

Positioning

Audience

⊕ = Approximate fit of my campaign



INNOVATIVE MEDIA (INFLUENCERS/SOCIALS)

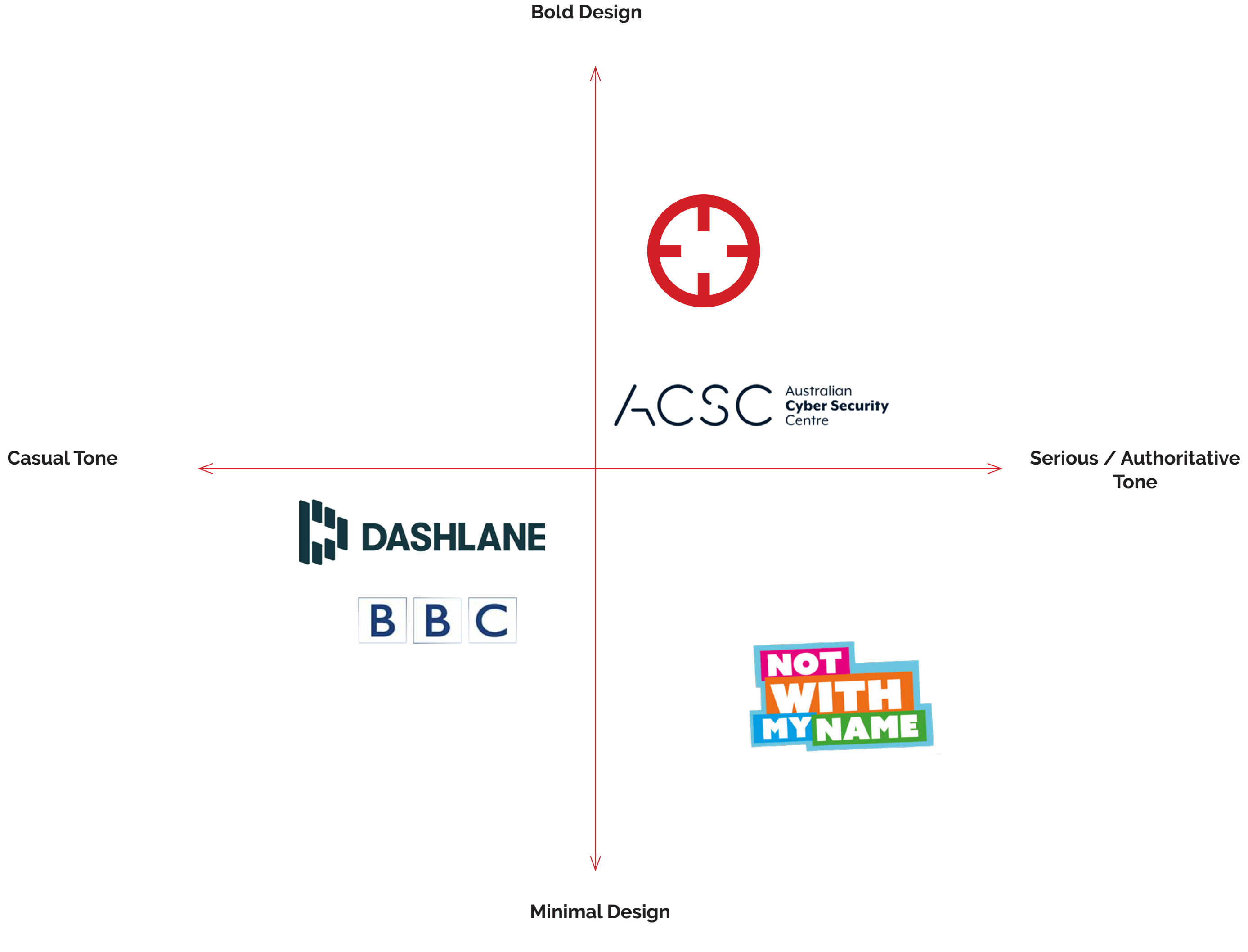
PROGRESSIVE, YOUNG AUDIENCE

OLDER, CONSERVATIVE PUBLIC

TRADITIONAL MEDIA (PRINT/RADIO/TV)

Positioning

Strategy



Bold Design

Casual Tone

Serious / Authoritative Tone

Minimal Design

Audience Research

Target Market

The target audience for the campaign will be comprised of two main areas:

Males & females aged 18-28 who are regularly exposed to scam texts, emails or pop up scam alerts. These are young, progressive thinkers and individuals who are regular users of online social platforms such as Instagram.

&

Males & females aged 45 - 65 who are older than the primary target audience, and are more vulnerable to falling victim to a scam. These individuals consume news and media through tv, radio, and news articles.

Audience Research Insights

In 2019, Australians under the age of 25 lost over $5 million to scams and reports made from this age group are increasing faster than older generations.

“Young people may think they are tech savvy, but scammers are adapting and we expect to see more scams on newer platforms such as Snapchat and TikTok.” (ACCC 2020).

People live increasingly online in 2023. It’s considered normal to create and use many accounts simultaneously across social platforms Instagram, Facebook and Youtube, just to name a few.

Due to the deceptive nature of scams, people are not always aware that they’ve been exposed to or responded to a scam, meaning, statistics could be even higher (ABS 2023). Most people do not know that personal data is always at risk when online.

Most people want easy seamless access to accounts, using the same password for everything. This however leaves data at risk.

Lockdowns and working from home have changed the way Australians use the internet, and the reliance on IoT devices, virtual classrooms, online communications, work, study and day-to-day life present new opportunities.

Persona

Primary Audience

Daniel

It would so gratifying to report a scammer. They shouldn't be able to have this much power and get away with their actions.

Age: 21 Years

Occupation: Retail employee / Student

Status: Single

Location: Melbourne, VIC

About:

Daniel is an avid user of all things tech. He loves to share his photography online, as well as game with his friends in his spare time.

Daniel's take on the issue:

As I have many social media accounts and accounts, I have to be mindful of the passwords I use. My details were recently exposed in a data breach, and I've been receiving a lot of scam texts these past few months. It's very frustrating and annoying having to deal with these messages as I am a busy person, and sometimes when I am tired after a long day of working, I don't really pay close attention when going through my phone. I've never felt so vulnerable about my private information, and now that it's out there, I could be a next target of a scammer. It's scary just thinking about how my information could be used to someone else's advantage.

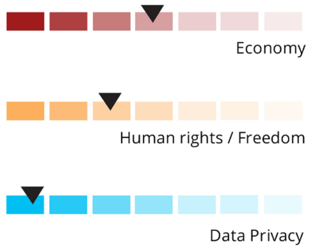
Goals:

- Wants an easy solution to report scam mesasages and phone calls
- As an individual with no power against scammers, Daniel wants to stop scammers and their malicious attacks. He wants to do everything he can.

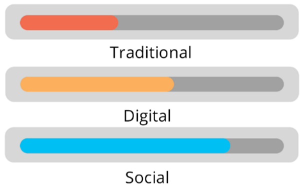
Frustrations:

- Uncertain how to report scam texts. (Do I call a hotline? How exactly do I report a scam?)
- Tough to manage scam texts and phone calls as a busy worker. He finds that trying to identify whether a text is a scam tactually takes up a lot of his time.

Issues I care about:



Media Channels:



The Process

- The Concept
- Design Development

The Concept

The campaign goal is to highlight the dangers and advancement of scams. The campaign, titled, ***'Use your scamera',*** is about creating awareness around evolving scams and establishing the next steps to be taken when exposed to scams in the form of identifying, capturing and reporting. Due to data breaches, many people experiencing feeling vulnerable having their personal information exposed, thus, it is important to empower people and implement a campaign people will find extremely useful and valuable.

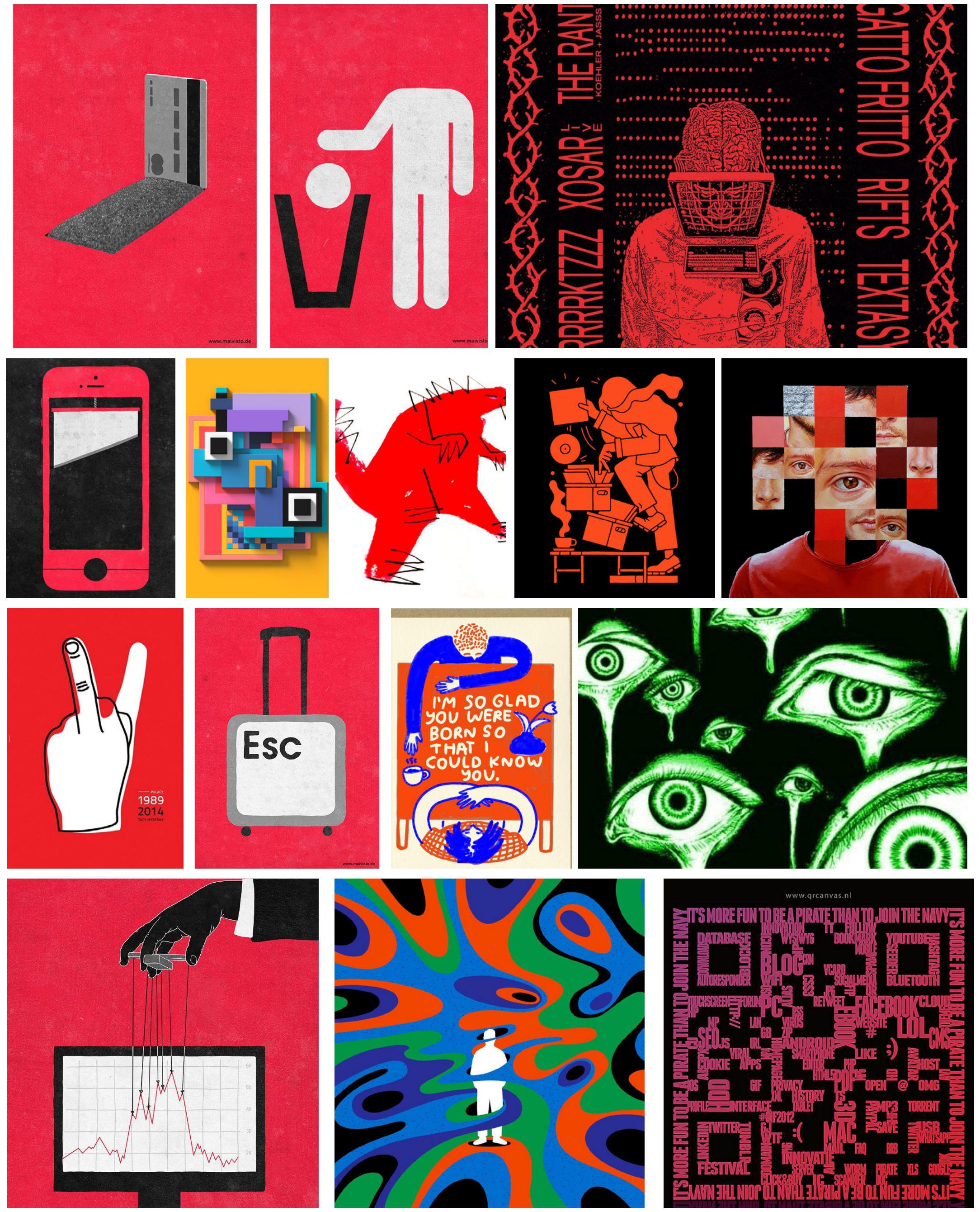
The campaign purpose is to prompt people to report suspicious phone numbers and capture screenshots of potential scams and upload them into the scamera mobile application or website. The social media posts on Instagram will highlight alarming statistics and alert the online community by sharing the newest scams which trick people through the use of humour and family members. Through instagram, polls, quizzes and stories can be implemented to engage the community. For example, asking them to guess which of the following is a scam, and build on their awareness of scams.

The tone of the campaign will be serious, intended to shock and urge people to take action against scams in the safest way possible.

This concept was chosen to be the most feasible, desirable and unique to competitors in the market.

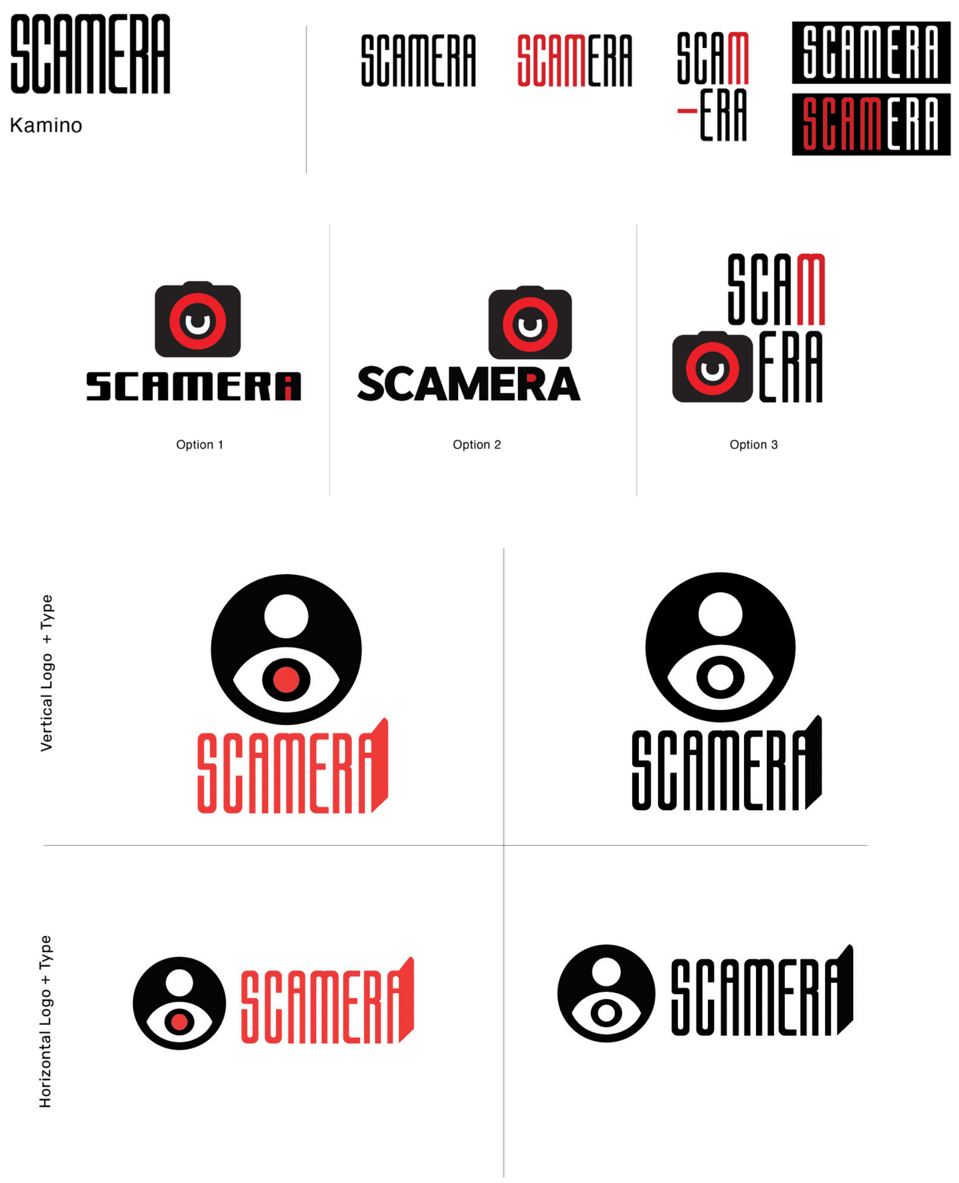
Design development

Moodboard


THE RANT
XOSAR
GATTO FRITTO RIFTS TEXTAS
Esc
I'M SO GLAD YOU WERE BORN SO THAT I COULD KNOW YOU.
1989
2014
IT'S MORE FUN TO BE A PIRATE THAN TO JOIN THE NAVY

Design development

Typography & Logo

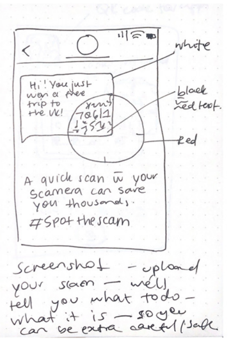


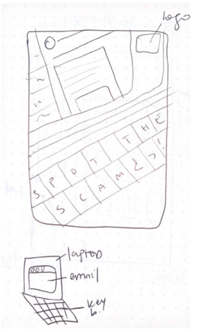
Refined Brandmark

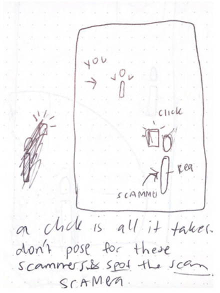
The refined logo utilises the icon figure in the centre, and incorporates an eye and a red recording symbol. The purpose of this logo is to signify that this involves scammers, and they're watching you. However, you could also look at it and think that the recording aspect can be a good thing, as scammers do not want their actions to be noticed/recorded. It sort of flips the narrative and symbolises the recording of the scammer, and with regards to the campaign objectives, it signifies that the people will not tolerate scams and they will now take charge and record/report the scammers.

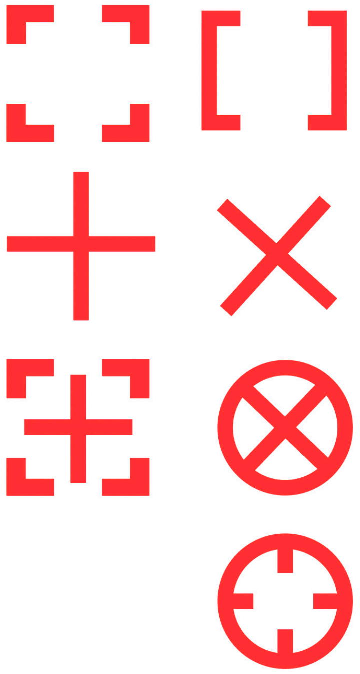
Design development

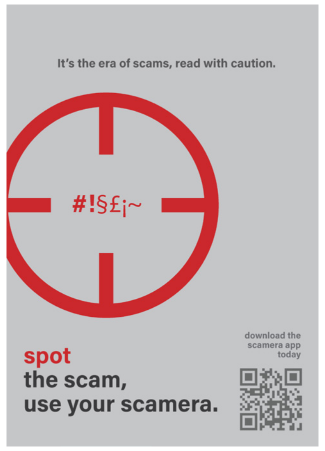
Poster Design & Graphics

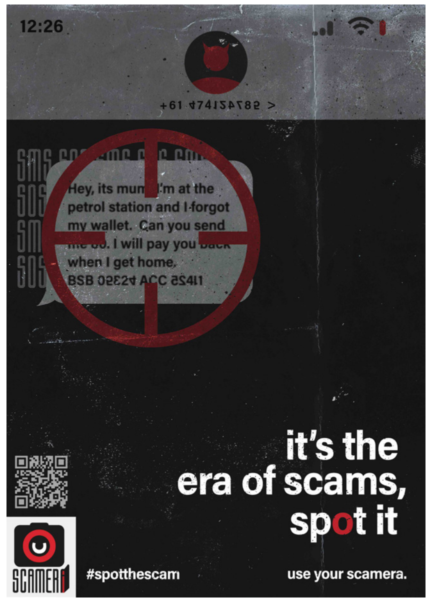

white
black
red text.
red
Hi! You just won a free trip to the UK!
A quick scan w your scamera can save you thousands.
#Spot the scam
Screenshot - upload your scam — we'll tell you what to do - what it is — so you can be extra careful/safe

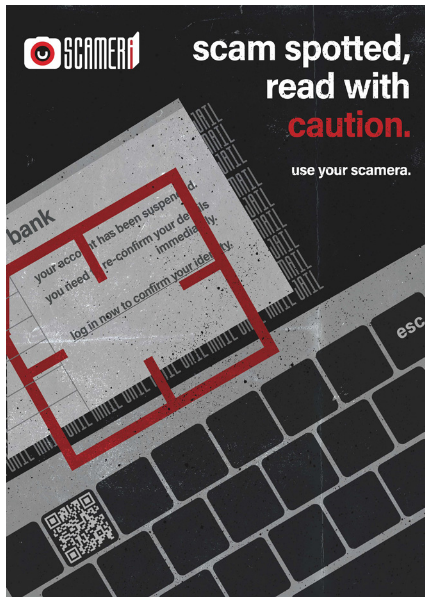


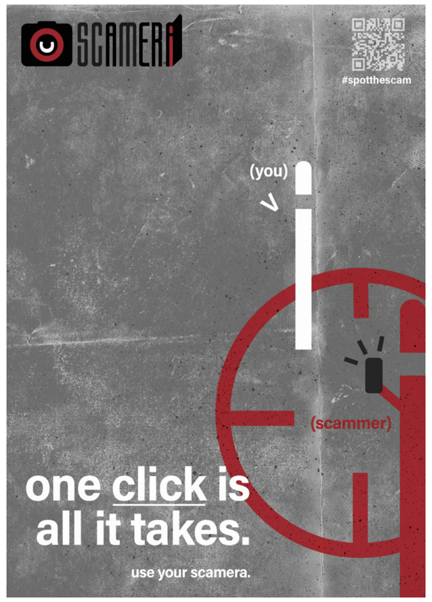





It's the era of scams, read with caution.
#!§£¡~
spot
the scam,
use your scamera.
download the scamera app today

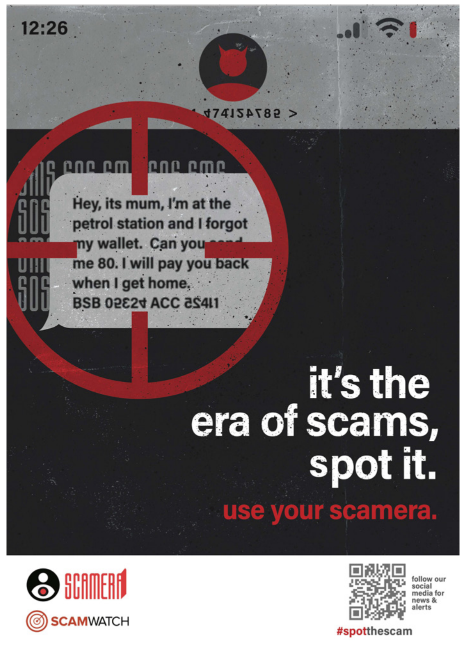

12:26
+61 474134782 >
Hey, its mum, I'm at the petrol station and I forgot my wallet. Can you send me 80. I will pay you back when I get home.
BSB 082824 ACC 825411
it's the
era of scams,
spot it
#spotthescam
use your scamera.

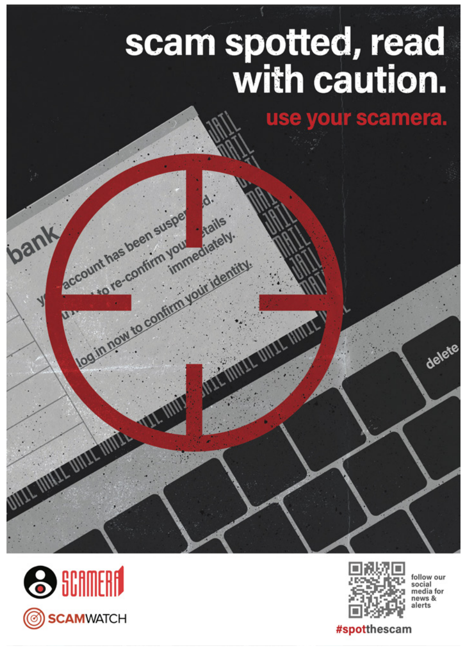

SCAMERA
scam spotted,
read with
caution.
use your scamera.
bank
your account has been suspended
you need to re-confirm your details immediately.
log in now to confirm your identity.
esc

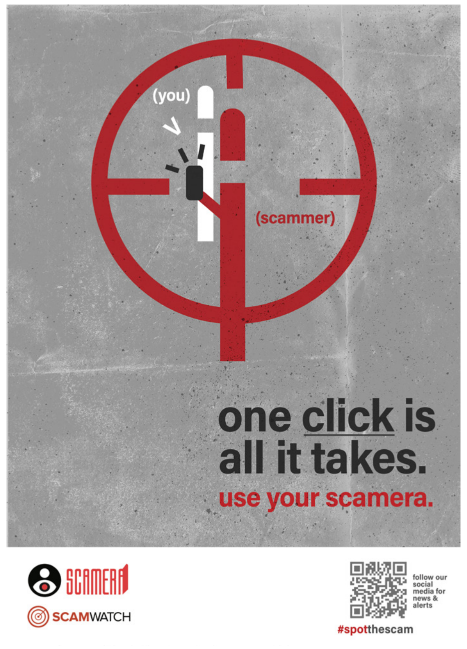


Design development

Refined Posters


12:26
474134782 >
Hey, its mum, I'm at the petrol station and I forgot my wallet. Can you send me 80. I will pay you back when I get home.
BSB 082824 ACC 825411
it's the
era of scams,
spot it.
use your scamera.
SCAMERA
SCAMWATCH
follow our social media for news & alerts
#spotthescam


scam spotted, read
with caution.
use your scamera.
bank
your account has been suspended.
you need to re-confirm your details immediately.
log in now to confirm your identity.
delete
SCAMERA
SCAMWATCH
follow our social media for news & alerts
#spotthescam

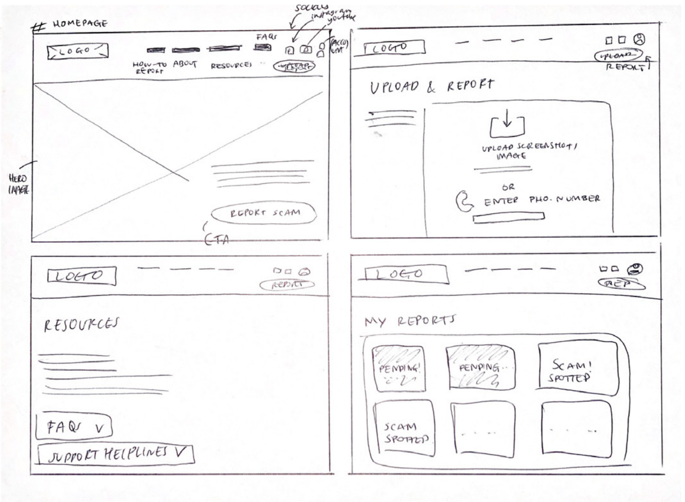


Poster mock-ups

A3 Posters were designed for the campaign to be distributed on bus-stop posts, billboards and large poster banners across metropolitan areas. The poster incorporates a QR feature that allows users to visit the Scamera social media profile on Instagram to keep track of the latest scams, alerts and statistics.

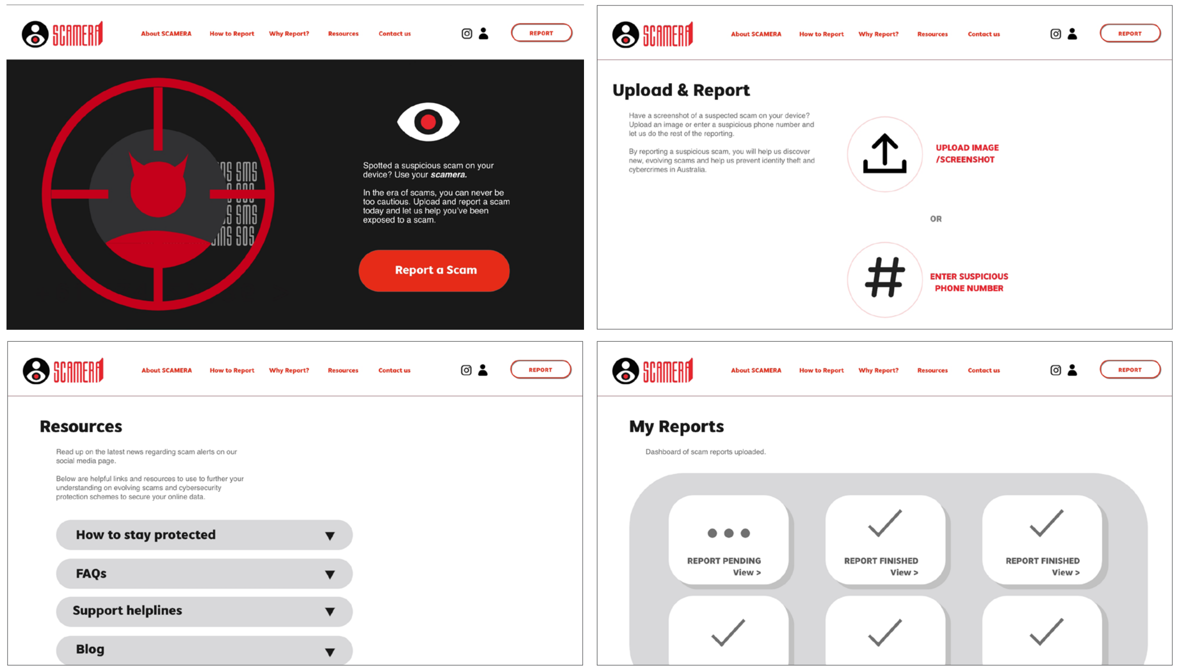
Design development

Website



Website wireframes

Wireframes for the pages 'Upload & Report', 'Resources', 'My Reports' and the main homepage of the scamera website was developed.



Spotted a suspicious scam on your device? Use your *scamera.*

In the era of scams, you can never be too cautious. Upload and report a scam today and let us help you've been exposed to a scam.

Upload & Report

Have a screenshot of a suspected scam on your device? Upload an image or enter a suspicious phone number and let us do the rest of the reporting.

By reporting a suspicious scam, you will help us discover new, evolving scams and help us prevent identity theft and cybercrimes in Australia.

Resources

Read up on the latest news regarding scam alerts on our social media page.

Below are helpful links and resources to use to further your understanding on evolving scams and cybersecurity protection schemes to secure your online data.

My Reports

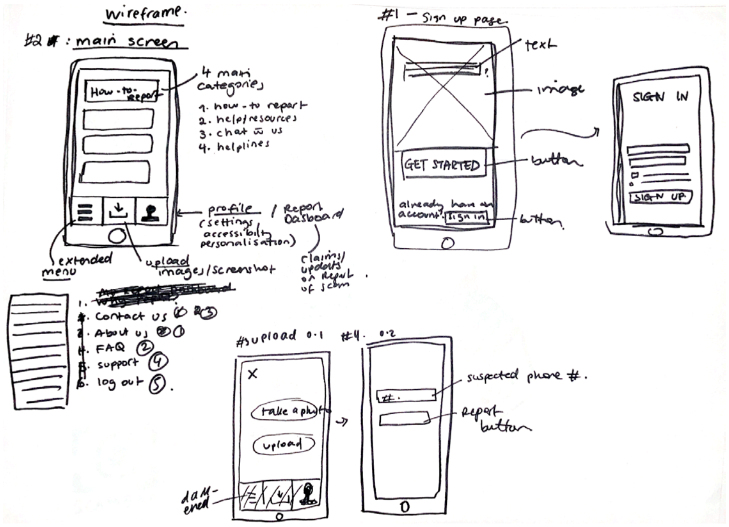
Dashboard of scam reports uploaded.

Website mock-ups

On the website, users can upload potential scams to check if they've recieved a scam message. The website offers support resources as well including hotlines, FAQs, blog articles and tips on how to stay protected online from scammers.

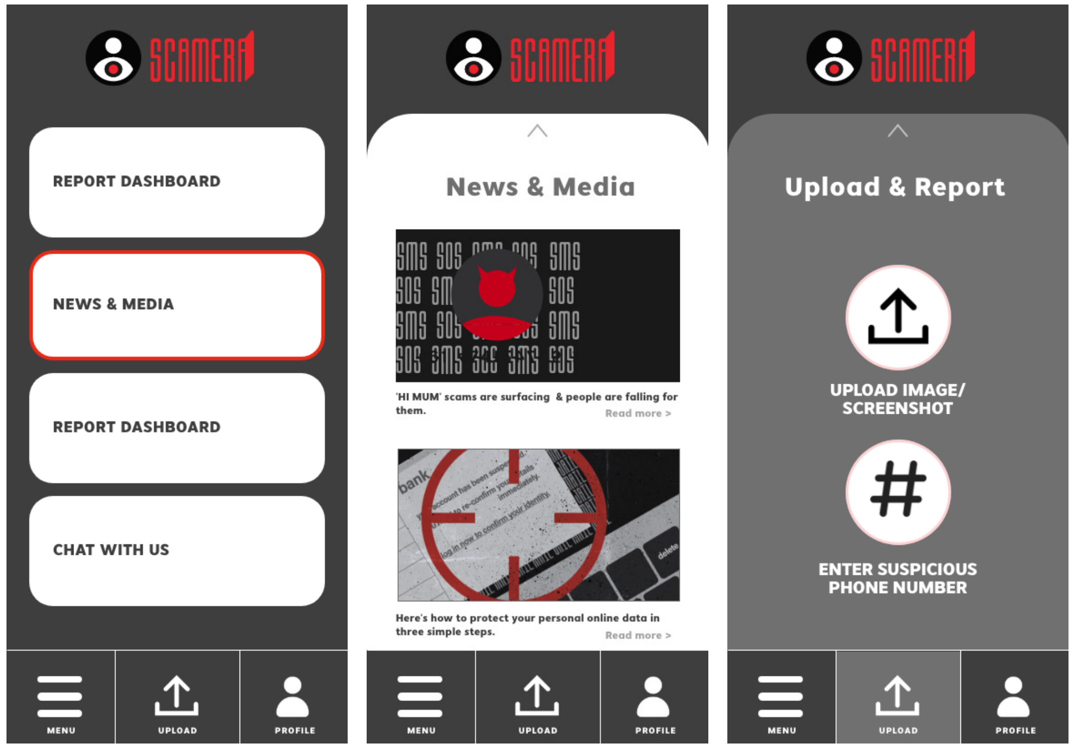
Design development

Mobile Application



App wireframes

Mobile App Design



'HI MUM' scams are surfacing & people are falling for them.

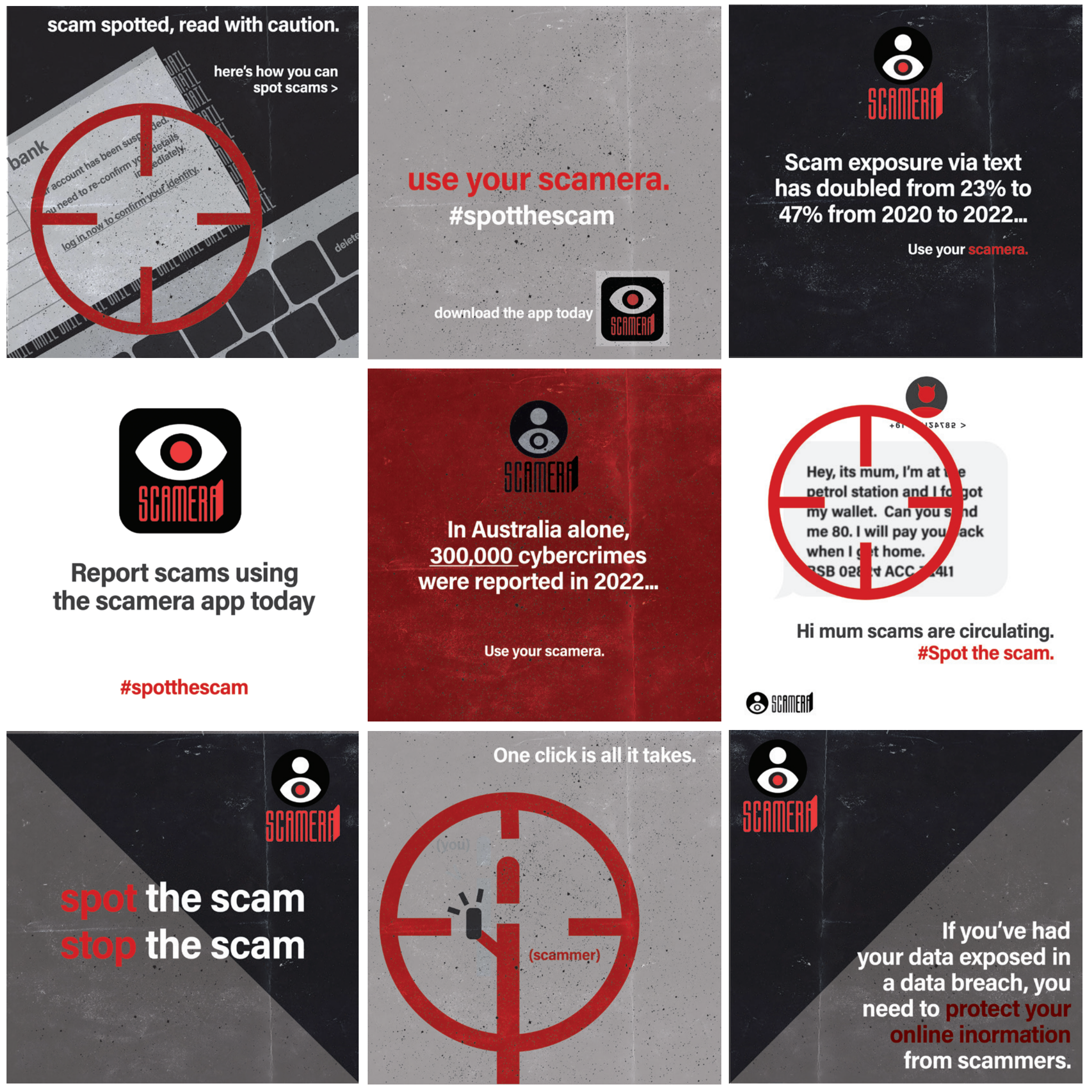
Here's how to protect your personal online data in three simple steps.

Mobile app mock-ups

An mobile app was designed for the campaign. This app will enable users of the app to upload and report suspicious text messages and scams, as well as browse news and media related to cybersecurity. Users, having uploaded and reported a scam screenshot or scam phone number, can check the status of their report claim on the dashboard, where the scamera app will inform users about the conditions of the report (blocked/stopped the number, identified scam in message, etc.)

Design development

Social Media

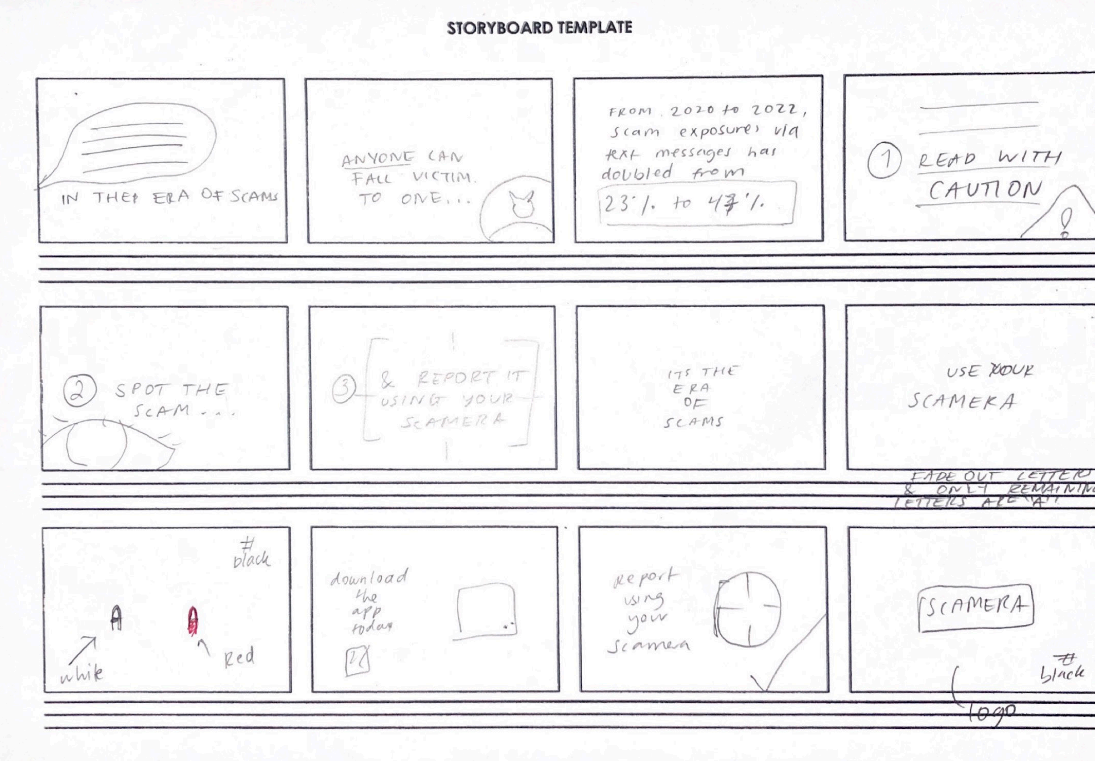

scam spotted, read with caution.
here's how you can spot scams >
bank
use your scamera.
#spotthescam
download the app today
SCAMERA
Scam exposure via text has doubled from 23% to 47% from 2020 to 2022...
Use your scamera.
Report scams using the scamera app today
#spotthescam
In Australia alone, 300,000 cybercrimes were reported in 2022...
Use your scamera.
Hey, its mum, I'm at the petrol station and I forgot my wallet. Can you send me 80. I will pay you back when I get home.
Hi mum scams are circulating.
#Spot the scam.
spot the scam
stop the scam
One click is all it takes.
(scammer)
If you've had your data exposed in a data breach, you need to protect your online inormation from scammers.

Social Media post mock-ups

On the main social media page hosted on Instagram, users can stay up to date with the latest scams in the media, read relevant news articles and blog material, learn how to stay safe online and be given insights into the situation through informative statistics. The social media page also utilises the hashtage #spotthescam and enables users of the social media app to share their scam stories.

Design development

Animation


STORYBOARD TEMPLATE
IN THE ERA OF SCAMS
ANYONE CAN FALL VICTIM TO ONE...
FROM 2020 to 2022, scam exposures via text messages has doubled from 23% to 47%.
① READ WITH CAUTION
② SPOT THE SCAM...
③ & REPORT IT USING YOUR SCAMERA
ITS THE ERA OF SCAMS
USE YOUR SCAMERA
FADE OUT LETTER & ONLY REMAINING LETTERS ARE 'A'
# black
white
red
download the app today
report using your scamera
SCAMERA
# black
logo

Animatic Storyboard sketch

Key frames and transitions are included in this storyboard sketch. It will feature statistics, the campaign name and tagline, and urge viewers of the animation to download the scamera app to identify and report scams.

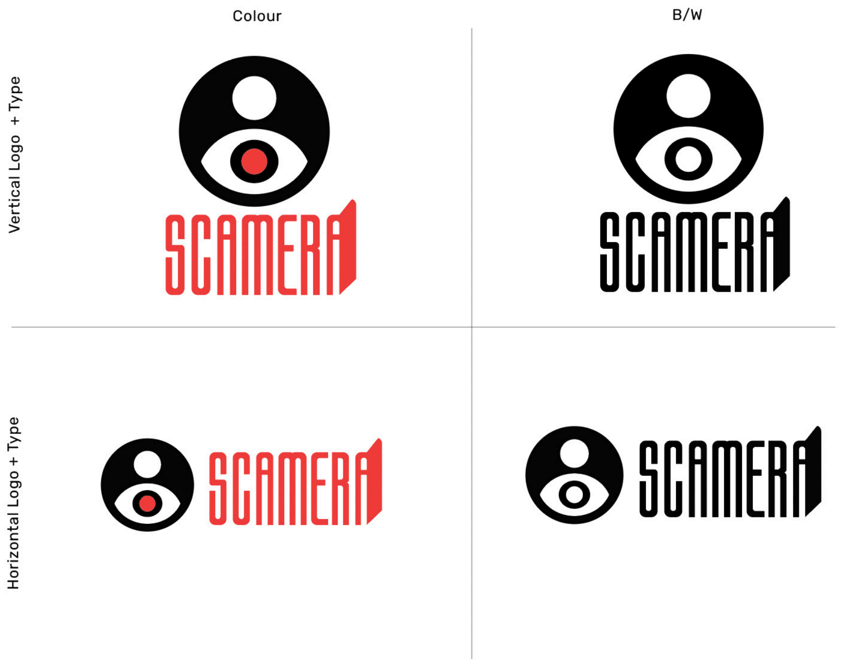
The Solution

- Final Branding
- Implementation mock-ups

Style Guide

Brand Identity

Final Brandmark



Colour Specifications

C 11 M 100 Y 100 K 3	C 0 M 0 Y 0 K 94	C 0 M 0 Y 0 K 20

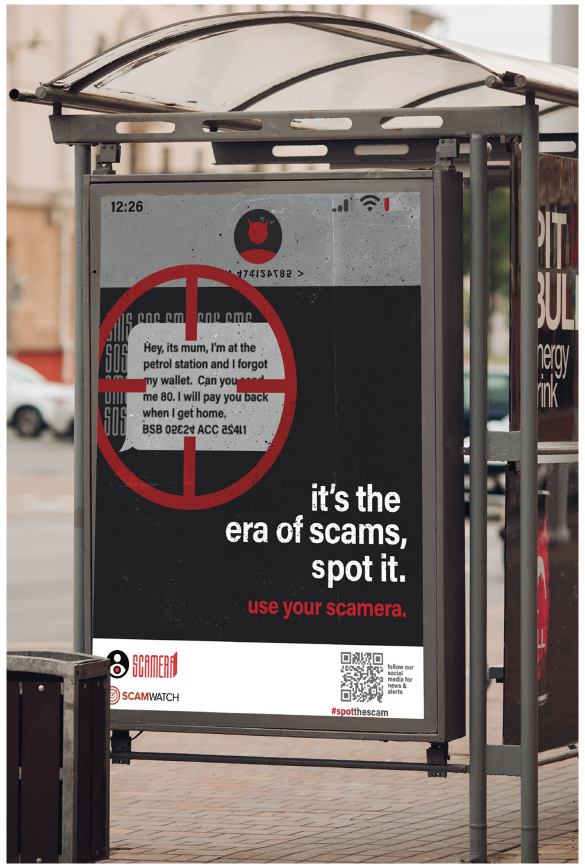
Typefaces

Acumin Variable Concept (Bold)
This font is the primary typeface used across all touchpoints including the poster designs, social media posts and short campaign animatic.

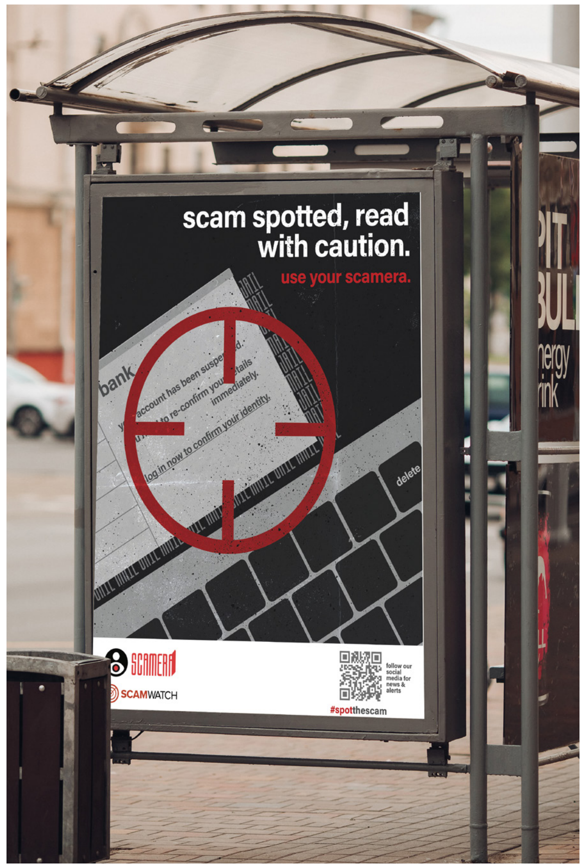
KAMINO
This font, Kamino, is the typeface used for the campaign brand mark. It utilises a custom font weight.

Implementation

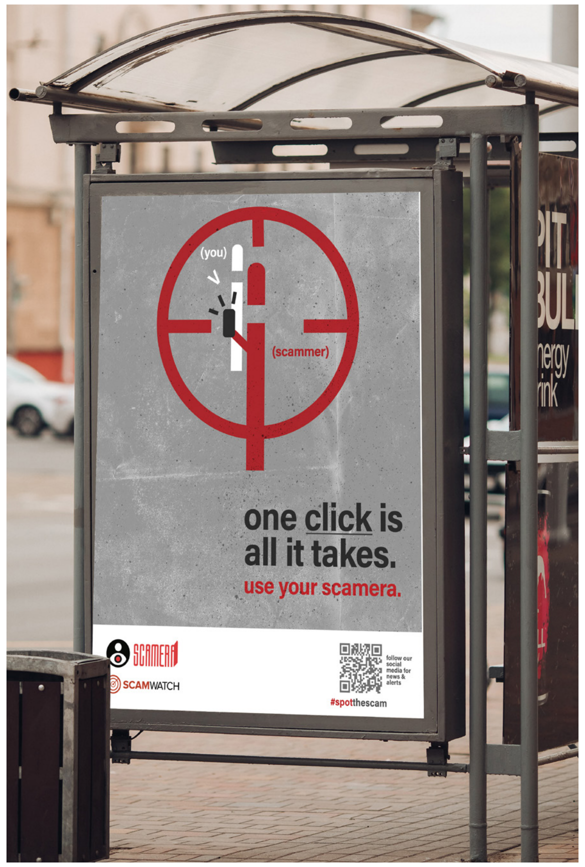
Campaign Poster



Hey, its mum, I'm at the petrol station and I forgot my wallet. Can you send me 80. I will pay you back when I get home.
BSB 02E24 ACC 2S411

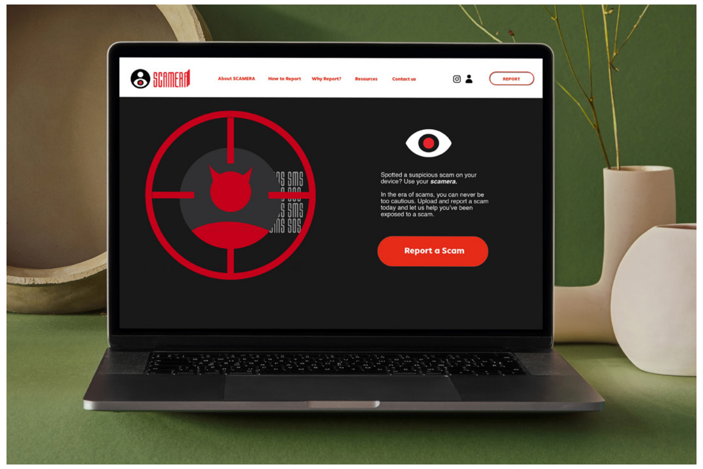


your account has been suspended.
you need to re-confirm your details immediately.
log in now to confirm your identity.



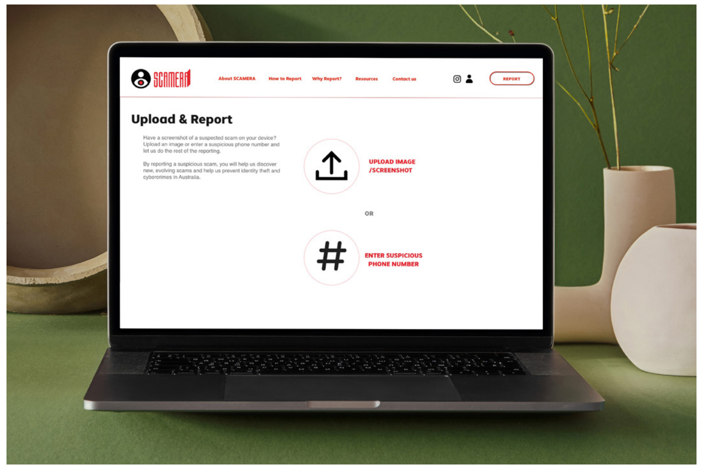
Implementation

Campaign Website



Spotted a suspicious scam on your device? Use your *scamera*.

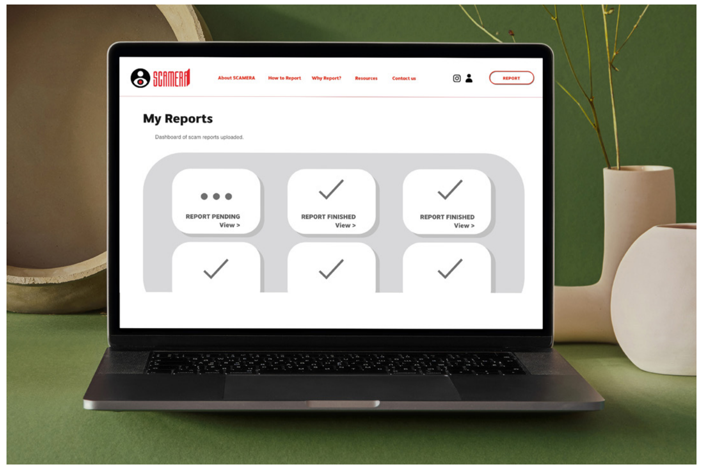
In the era of scams, you can never be too cautious. Upload and report a scam today and let us help you've been exposed to a scam.



Upload & Report

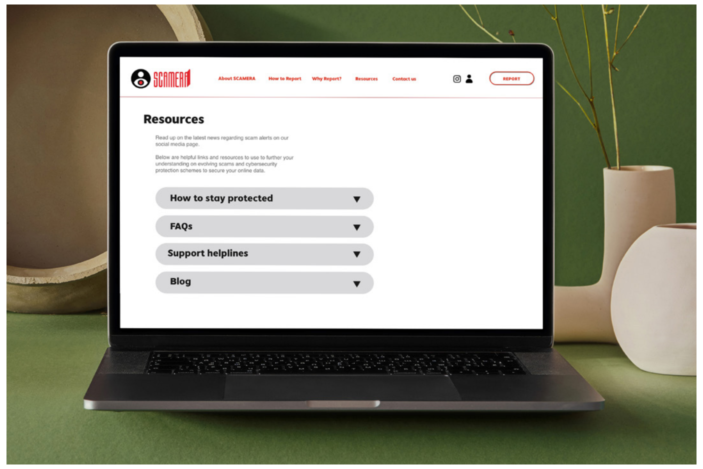
Have a screenshot of a suspected scam on your device? Upload an image or enter a suspicious phone number and let us do the rest of the reporting.

By reporting a suspicious scam, you will help us discover new, evolving scams and help us prevent identity theft and cybercrimes in Australia.



My Reports

Dashboard of scam reports uploaded.



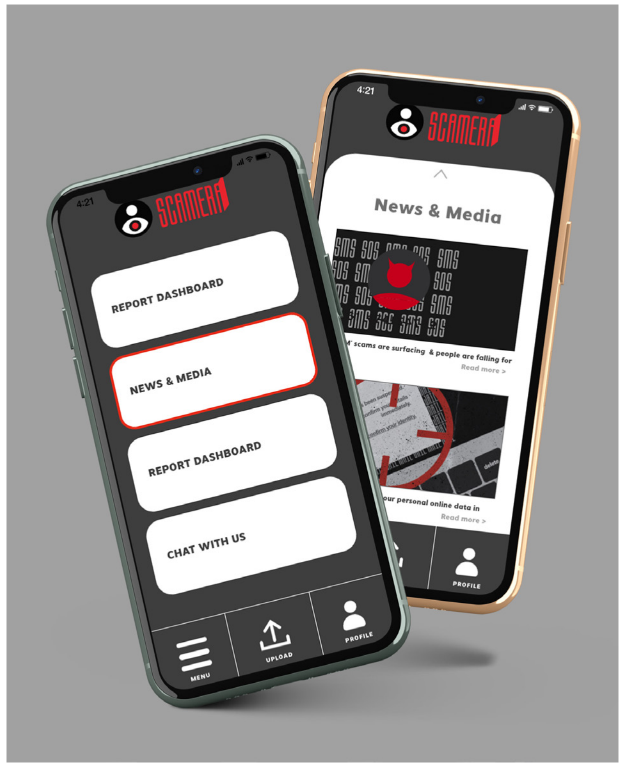
Resources

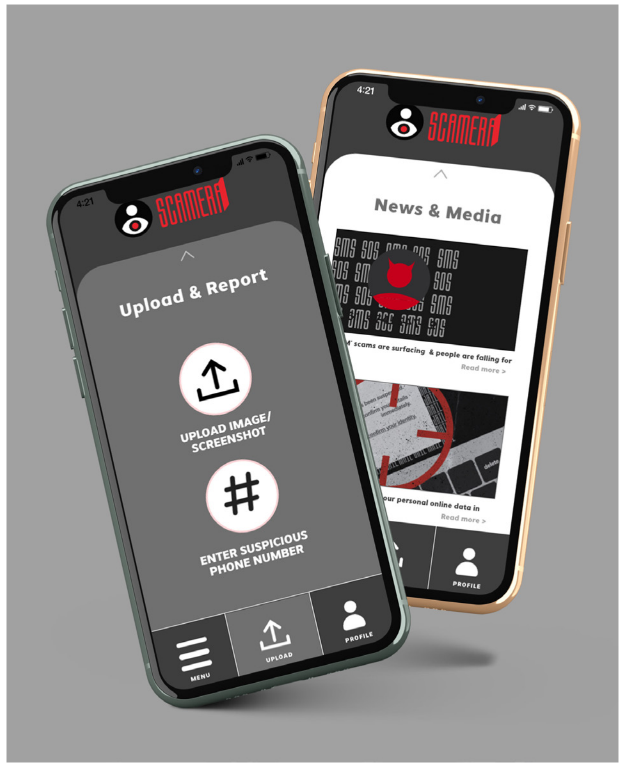
Read up on the latest news regarding scam alerts on our social media page.

Below are helpful links and resources to use to further your understanding on evolving scams and cybersecurity protection schemes to secure your online data.

Implementation

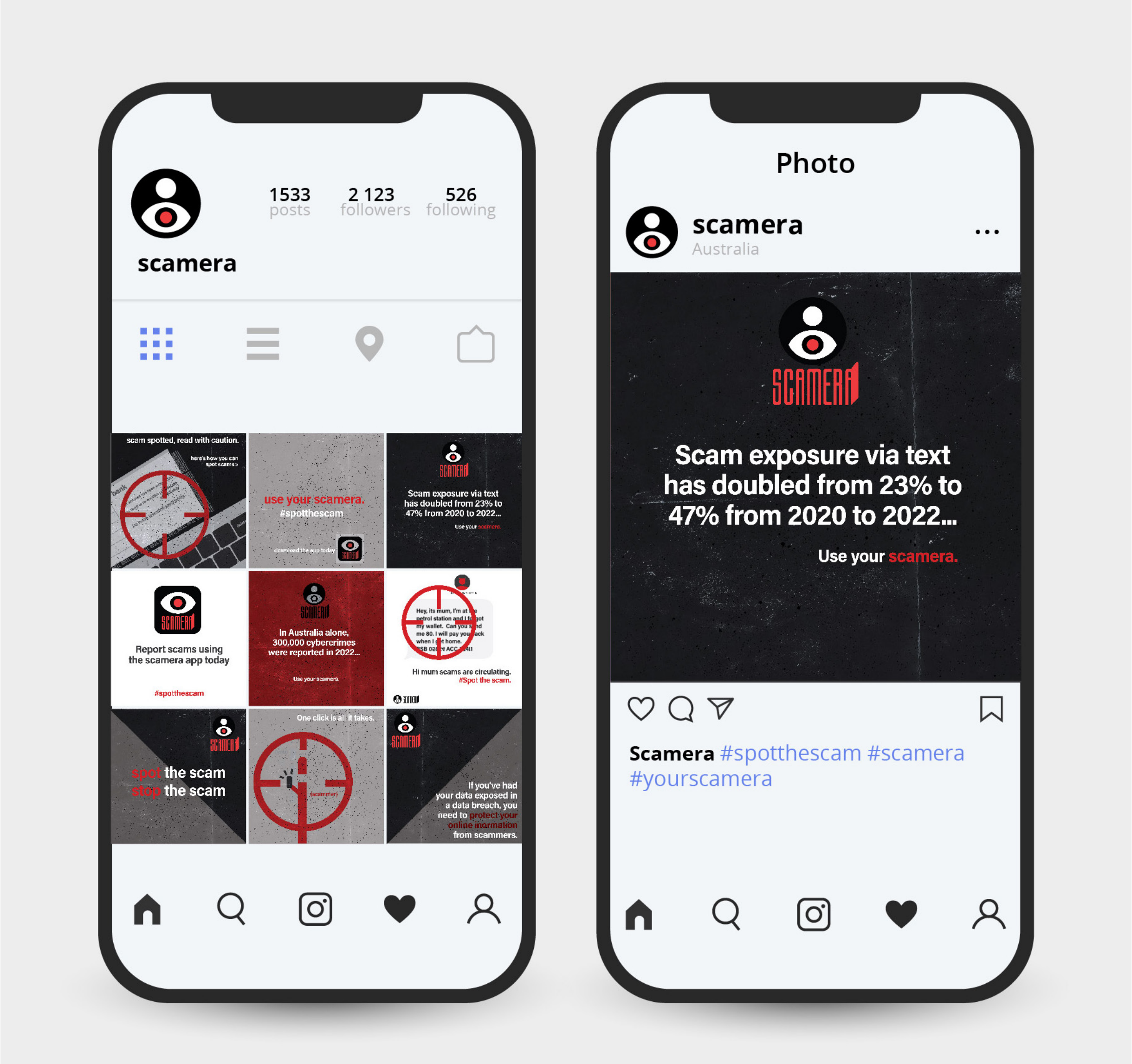
Campaign App





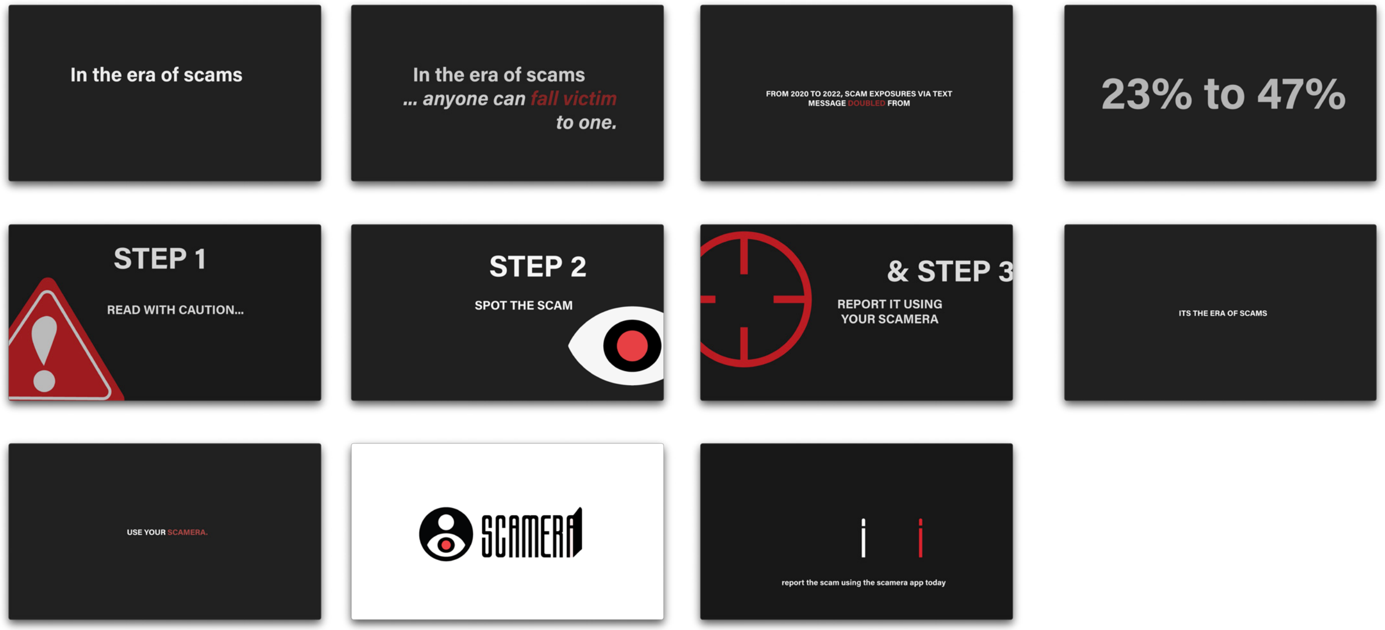
Implementation

Campaign Social Media


1533 posts
2 123 followers
526 following
scamera
Photo
scamera
Australia
SCAMERA
Scam exposure via text has doubled from 23% to 47% from 2020 to 2022...
Use your scamera.
Scamera #spotthescam #scamera #yourscamera
use your scamera.
#spotthescam
Report scams using the scamera app today
#spotthescam
In Australia alone, 300,000 cybercrimes were reported in 2022...
spot the scam
stop the scam
One click is all it takes.
#Spot the scam.

Implementation

Animation


In the era of scams
In the era of scams
... anyone can fall victim to one.
FROM 2020 TO 2022, SCAM EXPOSURES VIA TEXT MESSAGE DOUBLED FROM
23% to 47%
STEP 1
READ WITH CAUTION...
STEP 2
SPOT THE SCAM
& STEP 3
REPORT IT USING YOUR SCAMERA
ITS THE ERA OF SCAMS
USE YOUR SCAMERA.
SCAMERA
report the scam using the scamera app today

link to animation

https://vimeo.com/835428298?share=copy

Conclusion

By incorporting and combining multiple campaign medias to combat the growing issue of scams in Australia, this increases the chance of people taking up an offer for the greater good. As the campaign is targeted towards young adults, their passion and drive for positive change and reform will inspire a larger set of groups to take action. It was initially recognised that older groups aged 45-65 would be more susceptible to falling victims to scams, however, younger people are increasingly becoming affected as the years progress due to the evolving nature of scams and fraudulant notifications.

References

Research

ACCC 2020, 'Gen Z the fastest growing victims of scams', Australian Competition and Consumer Commission, viewed 13 April 2023, <https://www.accc.gov.au/media-release/gen-z-the-fastest-growing-victims-of-scams>.

Australian Bureau of Statistics 2021-22, Personal Fraud, ABS, viewed 13 April 2023, <https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2021-22>.

Broadhurst, R & Trivedi, H 2020, Trends & issues in crime and criminal justice Malware in spam email: Risks and trends in the Australian Spam Intelligence Database, viewed 13 April 2023, <https://www.aic.gov.au/sites/default/files/2020-09/ti603_malware_in_spam_email.pdf>.

Ellis, W 2023, 'Identity Theft Statistics (2023)', Privacy Australia, viewed 1 May 2023, <https://privacyaustralia.net/identity-theft-statistics/>.

Mondaca, G 2023, 'Critical Cyber Crime Statistics in Australia 2023', Eftsure, viewed 10 April 2023, <https://eftsure.com/en-au/statistics/cyber-crime-statistics/>.

Morris-Reade, R 2022, 'The rise of cybercrime - Over $300 million lost to scams last year', SecurityBrief Australia, viewed 13 April 2023, <https://securitybrief.com.au/story/the-rise-of-cybercrime-over-300-million-lost-to-scams-last-year>.

REINSW, 2022, 'The growing problem of identity theft (and what agents need to do about it)', Reinsw.com.au, viewed 13 April 2023, <https://www.reinsw.com.au/Web/News/Latest_News/2022/11-November/the-growing-problem-of-identity-theft-and-what-agents-need-to-do-about-it.aspx>.

Quinn, E 2022, 'How Common is Cyber Crime in Australia?, Ecu.edu.au, viewed 13 April 2023, <https://studyonline.ecu.edu.au/blog/how-common-cyber-crime-australia>.

Competitor Campaigns

Cyber.gov.au 2023, 'Cyber security campaign resources', Cyber.gov.au, viewed 14 April 2023, <https://www.cyber.gov.au/learn-basics/view-resources/cyber-security-campaign-resources>.

'Dashlane Super Bowl Commercial 2020: Password Pain! | Just Jared: Celebrity News and Gossip | Entertainment' 2020, Just Jared, viewed 14 April 2023, <https://www.justjared.com/2020/02/02/dashlane-super-bowl-commercial-2020-password-pain/>.

Gutteridge T, 2014, 'Corporate Comms', Behance, viewed 14 April 2023, <https://www.behance.net/gallery/21216341/Corporate-Comms>.

'Not With My Name Identity Crime Campaign | West Yorkshire Police' 2015, West Yorkshire Police, viewed 14 April 2023, <https://www.westyorkshire.police.uk/not-my-name-identity-crime-campaign>.

Sponsors

'Aura | Intelligent Digital Safety for the Whole Family' 2022, Aura.com, viewed 16 April 2023, <https://www.aura.com/>.

'Cyber Security | Australian Signals Directorate' 2021, Asd.gov.au, viewed 17 April 2023, <https://www.asd.gov.au/cyber-security>.

'eSafety Commissioner' 2022, eSafety Commissioner, viewed 17 April 2023, <https://www.esafety.gov.au/?gclid=CjwKCAjwhJukBhBPEiwAnilcNT-iv0nKxuWNooOkQUgEtm1Sv16NdEO524ZoBeU8sqoiwmlbEfS8JhoCTDcQAvD_BwE&gclsrc=aw.ds>.

'Home | Scamwatch', 2023, Australian Competition and Consumer Commission, viewed 17 April 2023, <https://www.scamwatch.gov.au/>.

'IDCARE Official Website | Identity Theft & Cyber Support' 2015, Idcare.org, viewed 17 April 2023, <https://www.idcare.org/>.

Moodboard / Inspiration

'Identity Theft' 2013, Pinterest, viewed 1 May 2023, <https://www.pinterest.com.au/altiparmakseren/identity-theft-campaign-moodboard/>.

Illustrations / Designs

'QR Code Generator | Create Your Free QR Codes' 2019, Qr-code-generator.com, viewed 1 June 2023, <https://www.qr-code-generator.com/>.

Persona / Roleplay

Cameron, JM 2020, 'Photo of Woman and Boy Sitting on Couch · Free Stock Photo', Pexels, Pexels, viewed 20 April 2023, <https://www.pexels.com/photo/photo-of-woman-and-boy-sitting-on-couch-4145352/>.

Schnagl, T 2020, 'Man in Brown Coat and Black Cap · Free Stock Photo', Pexels, Pexels, viewed 20 April 2023, <https://www.pexels.com/photo/man-in-brown-coat-and-black-cap-5588224/>.

Sharma, C 2017, 'User Persona & Scenario Template: FREE DOWNLOAD', Behance, viewed 20 April 2023, <https://www.behance.net/gallery/56953021/User-Persona-Scenario-Template-FREE-DOWNLOAD>.

'Values Segments - Roy Morgan Research' 2022, Roymorgan.com, viewed 19 April 2023, <https://www.roymorgan.com/products-and-tools/values-segments>.

Mockups

'Realistic instagram photo frame on smartphone Free Vector' 2019, Freepik, viewed 3 June 2023, <https://www.freepik.com/free-vector/realistic-instagram-photo-frame-smartphone_4264406.htm#query=iphone%2013%20mockup&position=7&from_view=keyword&track=ais>.

'Free MacBook Pro with Vase Mockup' 2023, Dribbble, viewed 4 June 2023, <https://dribbble.com/shots/19029781-Free-MacBook-Pro-with-Vase-Mockup>.

'Free Phone App Presentation Mockup' 2020, Free Design Resources, viewed 4 June 2023, <https://freedesignresources.net/free-phone-app-presentation-mockup/>.

IOS 14 Homescreen, Reddit, viewed 4 June 2023, <https://i.redd.it/u01427dqvlr41.png>.

'A large billboard with interesting information and advertising on it installed along a wide street in the city center Free PSD' 2020, Freepik, viewed 6 June 2023, <https://www.freepik.com/free-psd/large-billboard-with-interesting-information-advertising-it-installed-along-wide-street-city-center_9016091.htm#query=bus%20stop%20mockup&position=0&from_view=keyword&track=ais>.

Animation

Music from #Uppbeat (free for Creators!):
https://uppbeat.io/t/kevin-macleod/lightless-dawn
License code: DHYJLVRFKSBZNPMC