# Scam Analysis Report

## Identifying Emerging Fraud Patterns to Support Data-Driven Insights for Building an AI Solution for Scam Reduction

Nay Chi Than Shwe

November 2025

# Table of Contents

# Report Overview

This project analyses **ScamWatch data (2020 – 2024)** to uncover key trends and risk patterns in consumer scams across Australia. The objective is to **understand the most common scam types, most affected demographics, and contact channels** to inform the design and implementation of an **AI-driven scam detection and prevention solution** using AWS services. This analysis forms the foundational research phase of a comprehensive AI solution portfolio project.

# Background & Motivation

During industry research, financial institutions consistently identified scams and fraudulent activities as one of their most pressing challenges. This portfolio **project aims to demonstrate how AI and cloud technologies can be applied to address this real-world problem through data-driven solution design.**

The ScamWatch dataset, **published by the Australian Competition and Consumer Commission (ACCC)**, offers publicly available, large-scale records of reported scams, including scam category, contact mode, demographics, and financial loss value.

This analysis **serves as the data exploration and problem definition phase**, establishing the evidence base for designing an AI-powered scam detection system using AWS services.

# Objectives

- Analyse **scam types and their evolution** over time.
- Assess the impact of **different contact modes** (e.g., phone, text, email, social media) and their trends over time.
- Identify the **demographics** most affected by scams.
- Provide insights to determine **which demographics and contact channels should be prioritised** in an AI-driven approach to reduce scam risks and financial losses.

# Methodology

## Data Collection

**Primary Dataset:** Scam report data was obtained from the ScamWatch platform, administered by the Australian Competition and Consumer Commission (ACCC). ScamWatch is a publicly accessible repository where Australian consumers voluntarily report scam incidents. The dataset was downloaded in CSV format and covers reports from January 2020 to March 2025. However, only complete calendar years (2020-2024) were included in the analysis to ensure balanced year-over-year comparisons.

**Supplementary Data:** Population statistics for Australian states and territories were sourced from the Australian Bureau of Statistics (ABS) to enable normalised per capita loss calculations across regions.

**Ethical Considerations:** As the ScamWatch dataset consists of publicly available, de-identified consumer reports with no personally identifiable information, formal ethical approval was not required. All data was aggregated at the group level for analysis, with no individual-level identification possible.

## Data Analysis Methods

**Data Processing:** Raw data was processed using SQL Server Management Studio (SSMS). This included consolidating quarterly datasets, standardising data formats, handling missing values, and restructuring the data using dimensional modelling techniques (star schema) to optimise analytical performance.

**Statistical Analysis:** Descriptive statistics were calculated to identify patterns in scam frequency, financial losses, and demographic distributions. Year-over-year comparisons were performed to identify temporal trends.

**Visualisation and Exploration:** Power BI Desktop was used for data visualisation and interactive analysis. This enabled dynamic exploration of multi-dimensional patterns across time, geography, scam type, and demographics.

## Tools and Software

**SQL Server Management Studio (SSMS):** Used for data consolidation, cleaning, transformation, and normalising tables.

**Power BI Desktop:** Used for data validation, relationship modelling, DAX measure creation, and dashboard development. Power Query Editor within Power BI was used for data profiling and quality verification.

## Justification

The combination of SQL and Power BI was selected for its complementary strengths. SQL provides robust capabilities for handling large datasets and performing complex transformations.

**Data normalisation** was applied to improve **reusability, scalability, and long-term maintainability of the dataset.** By structuring the data into dimensional tables (scam types, contact methods, age groups, and regions) linked to a central fact table, the model becomes more efficient for queries, easier to update, and adaptable for future analysis requirements.

**Power BI enables interactive visualisation and dynamic exploration** of patterns that may not be immediately apparent through static analysis.

## Limitations

Several limitations should be noted. The ScamWatch dataset **represents only reported scams and likely underestimates total scam activity,** as many incidents go unreported. The data relies on self-reported information, which may be subject to recall bias or incomplete details. The dataset provides limited demographic information (age, region and gender only), **lacking other potentially relevant factors such as education level, employment status, income, or digital literacy.**

# Executive Summary

**Most Common Scam Type**

**Phishing** accounts for **30.79%** of total reports but contributes only **4.31%** of total financial losses.

**Highest Financial Loss Scam Type**

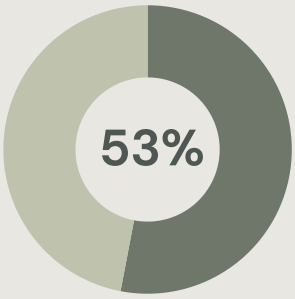
**Investment scams** make up just **3.2%** of total reports but cause **52.59%** of total financial losses.

**Emerging Scam Contact Mode**

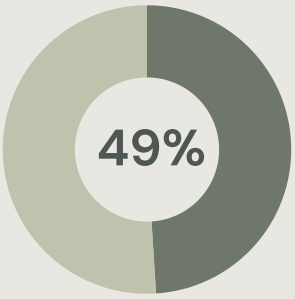
**Phone calls** led until 2021 but have since **declined sharply**, while **email scams** rose from **2.95% to 6.68% between 2021 and 2024.**

**Most Affected Age Group**

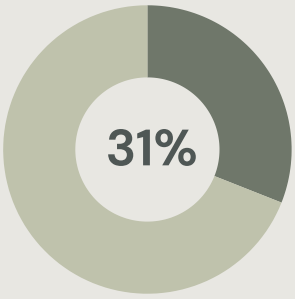
The **55+** age group accounts for **42.39%** of total reports, making it the most affected demographic.




52% of total financial loss from investment scams




49% financial loss from ages 55+




51% of total reports are phishing

This report **analyses ScamWatch data from 2020 to 2024** to **uncover emerging scam patterns across Australia** and inform the **design of an AI-driven scam detection solution.** The findings show that **phishing is the most commonly reported scam type,** accounting for nearly **one-third of all reports**, while **investment scams** remain the most f**inancially damaging, contributing more than half of the total losses** despite representing a small share of reports.

Scam contact methods have shifted significantly over time. **Phone calls dominated scam activity in 2020;** however, by **2024** scammers increasingly relied on digital channels, particularly **text messages and email**. Phishing scams now primarily occur through these digital channels, while investment scams continue to rely heavily on phone calls.

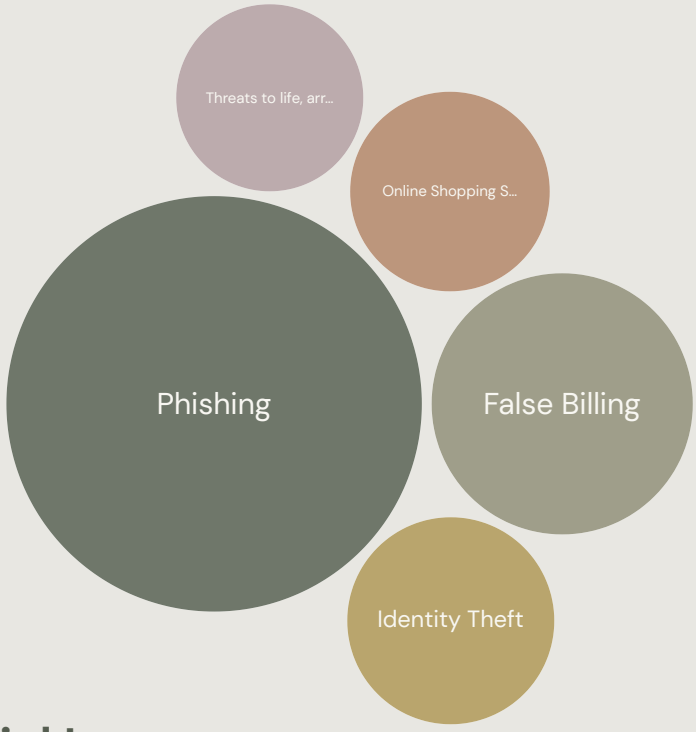
Demographically, individuals **aged 55 and above represent the highest-risk group,** with those aged 65 and over experiencing both the highest number of reports and the highest financial losses. The analysis further reveals that **males incur substantially more financial loss than females, largely due to higher exposure to investment scams**.

These insights inform the development of a **targeted AI solution using AWS services**, designed to detect and prevent sophisticated phishing attacks across email and text message channels, with **particular focus on protecting high-risk demographic groups.**

# Key Insights

## Top 5 Scam Types By Number of Reports

- **Phishing** is overwhelmingly the **most reported scam type**, far exceeding all other categories.
- **False Billing, Online Shopping Scams, and Identity Theft follow behind** but at much lower volumes.
- This indicates that **high-volume scam types are not always the ones causing the highest financial loss**, as shown in the next chart.




## Top 5 Scam Types By Financial Loss


- **Investment scams cause the most financial loss** by a wide margin, despite making up only a small share of total reports.
- **Phishing, Dating & Romance, and False Billing contribute significantly less** financial impact.
- This demonstrates that scam types with **fewer victims can still cause the most severe financial harm.**

# Top 5 Scam Contact Methods



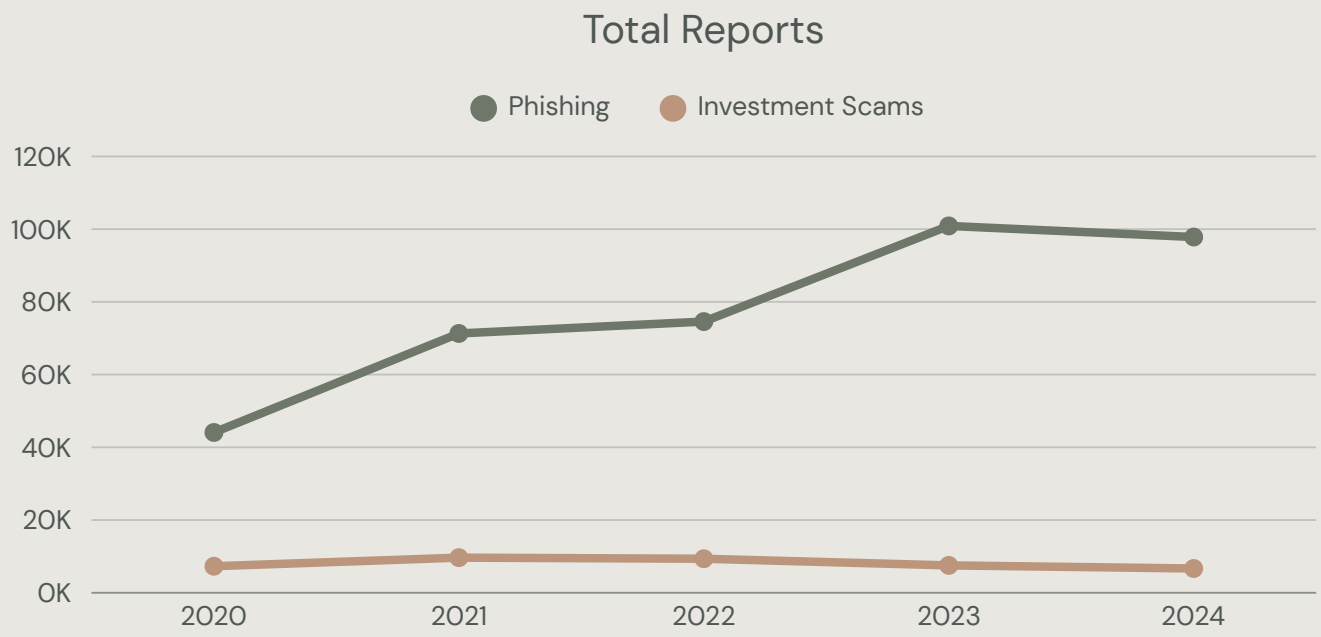
- **Phone calls dropped** sharply from being the dominant contact method in 2020 to one of the least common in 2024.
- **Email and text message** scams grew significantly, with email becoming the **leading contact method by 2024.**
- **Social media/online forums** also increased steadily, reflecting scammers **shifting towards digital channels.**
- Overall, scammers are moving away from traditional phone calls and **increasingly using digital communication methods.**

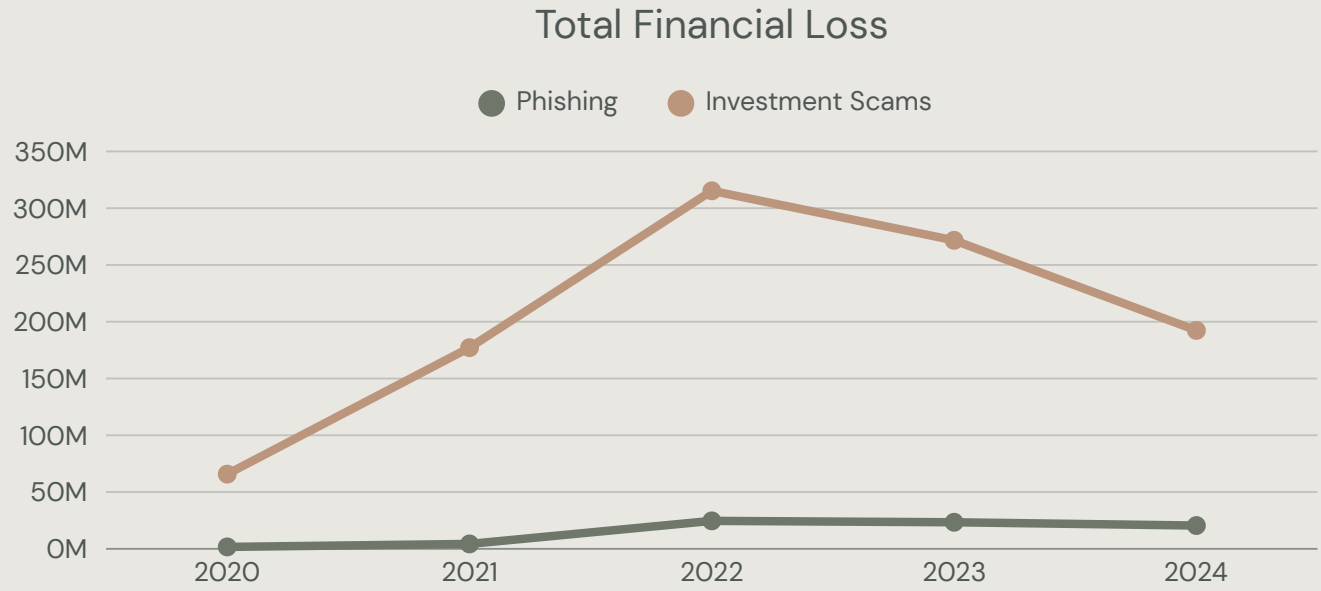
# Top Contact Methods For Most Impactful Scam Types



The two bar charts above show a clear shift in scam contact methods between 2020 and 2024. In 2020, phone calls were the most common contact method for both phishing and investment scams. By 2024, **email and text message contact** for **phishing increased** significantly, making text messages the most common methods for phishing. For i**nvestment scams, phone calls remained the dominant method** in both years, while contact via text message was almost non-existent.

Overall, the number of investment scam reports has been declining, whereas **phishing reports have continued to rise.** This indicates that **mitigation efforts should priorities filtering phishing attempts**, particularly those delivered through text messages and email.

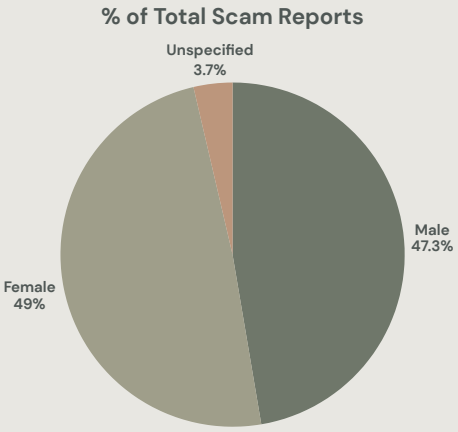


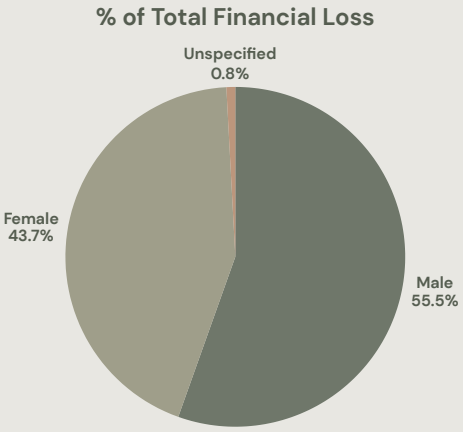




The two figures above highlight the most impactful scam types. **Phishing affects** the **largest number of people**, while i**nvestment scams result in the highest financial losses**. From 2020 to 2024, **phishing reports have increased steadily** each year, whereas **investment scam reports have gradually declined** during the same period.

In terms of financial loss, **investment scams reached a peak of 315.29 million dollars in 2022** and **decreased to 192.35 million dollars in 2024**. Although **phishing** results in far lower financial loss, its impact has g**rown significantly over time,** rising **from 1.69 million dollars in 2020 to 20.51 million dollars in 2024**. Overall, investment scams cause much greater financial loss, but phishing affects more individuals and continues to increase each year.

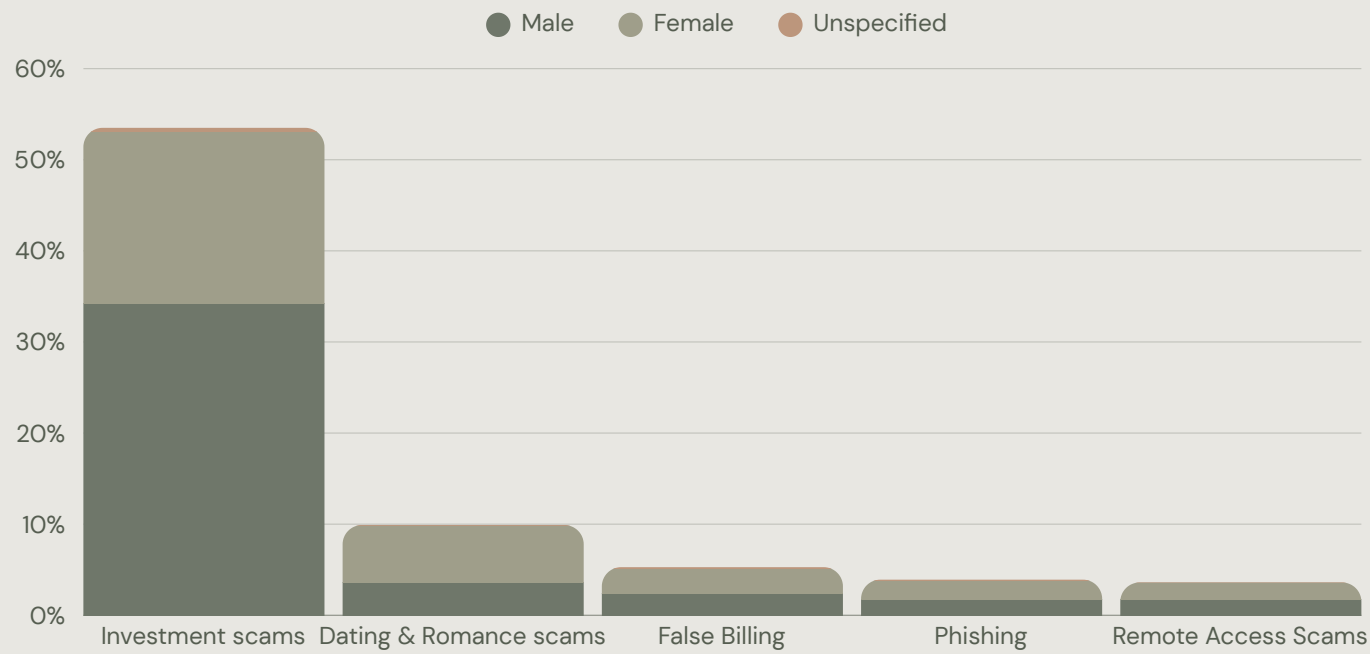
# Detailed Demographic Analysis




The pie charts on the left show that **females report** scams **more frequently,** whereas **males incur higher financial losses**. The bar chart below illustrates the factors contributing to this difference.

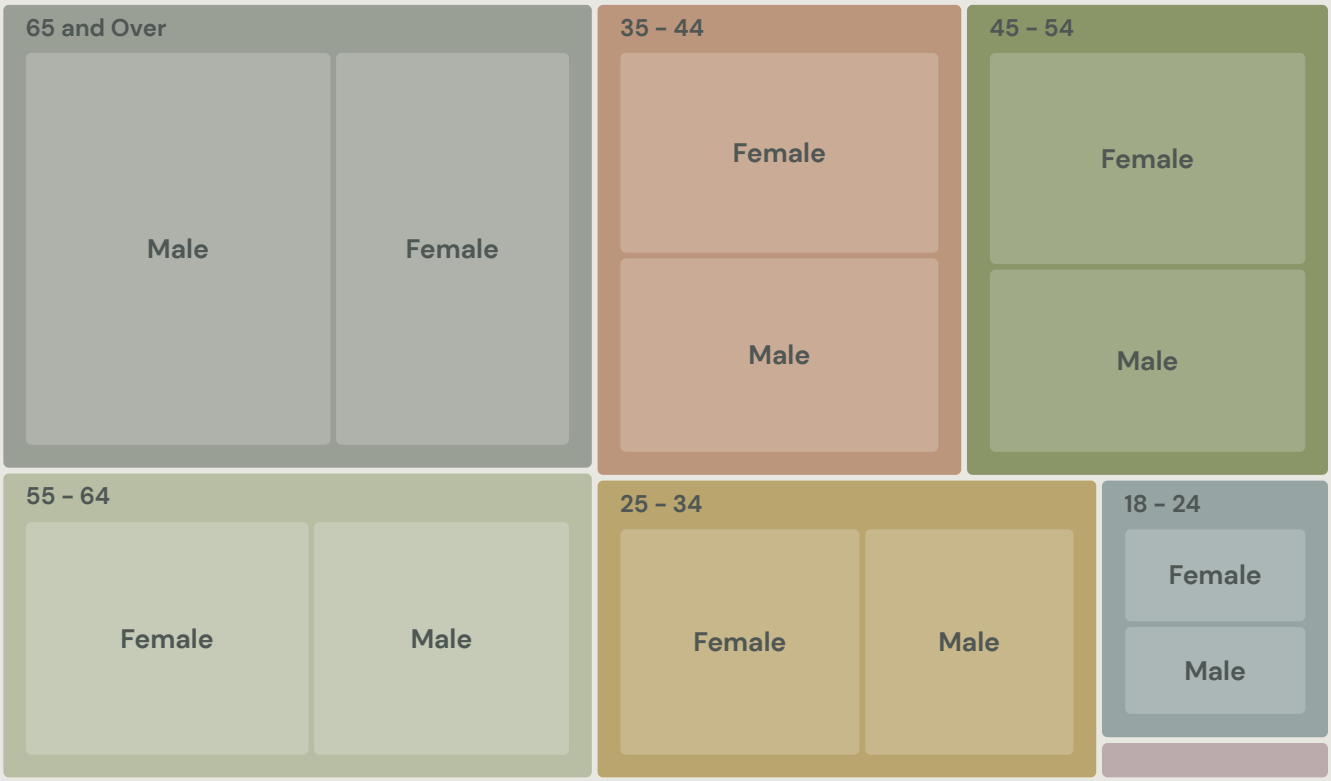
## Gender Breakdown of Total Loss Across Top 5 Scam Categories




This figure shows that **males lose 15.28%  more than females in investment scams.** Investment scams account for **over 50% of total financial loss** for both genders, while the second highest category, **dating and romance scams**, accounts for only **about 10% of total loss.**

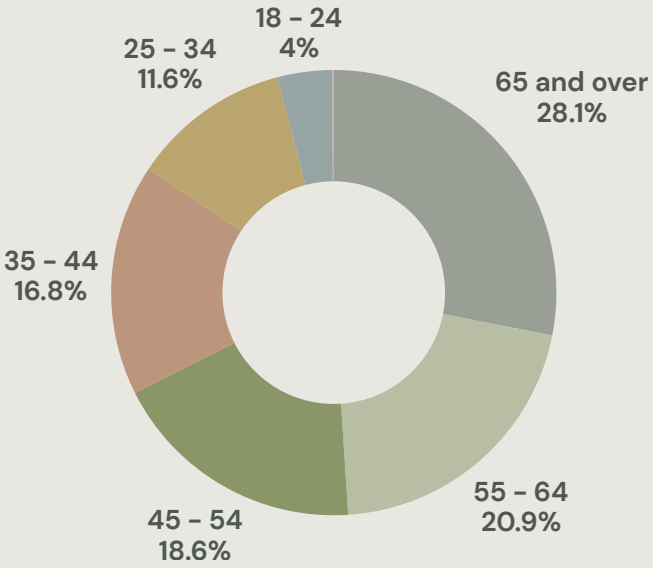
Aside from investment scams, **females lose slightly more than males** in most **other scam types**. This disproportionate impact from investment scams helps explain why females report more scams overall while males experience greater financial losses.

## Total Reports




As shown in the treemap above, individuals **aged 65 and over,** followed by those **aged 55 to 64**, are among the **most frequently targeted** groups. Together, these two age groups account for around 420,505 reports, which is **approximately 80%** of the 521,422 reports from **all other age groups combined.** While other age groups show little difference between male and female victims, **the 65 and over group has noticeably more males affected than females**.

## Total Financial Loss




Similarly, for **financial loss**, individuals **aged 65 and over experience the highest losses**. When combined with those aged **55 to 64**, these **two age groups account for 49% of the total financial loss.**

# Conclusion

## Key Findings from Data

This analysis of ScamWatch data from 2020 to 2024 reveals three critical patterns that should inform scam prevention strategies in Australia.

First, **phishing has emerged as the main threat by volume, accounting for 30.79%** of all reported scams. While contributing only **4.31% of total financial losses**, its impact has grown substantially, with losses increasing from **$1.69 million in 2020 to $20.51 million in 2024** which is a twelve-fold increase.

Second, scam contact methods have gone through a fundamental shift. **Phone calls declined sharply from 103,000 reports in 2020 to just 41,742 in 2024.** In contrast, email and text message scams increased dramatically, **with email rising from 32,337 to 90,819 reports. By 2024, phishing was overwhelmingly delivered through these digital channels.**

Third, individuals **aged 55 and above represent the highest-risk group, accounting for 42.39% of all reports and 49% of total financial losses.** The data further reveals that **males experience substantially higher financial losses,** primarily due to greater exposure to **investment scams.**

## Industry Trends

The patterns observed in ScamWatch data align with broader cybersecurity developments. **Phishing** attacks are no longer simple mass-mail scams. They have **become highly personalised, context-aware, and increasingly powered by generative AI.**

Attackers now use **generative AI to mimic legitimate communication styles**, creating significantly more convincing messages. Phishing-as-a-Service (PhaaS) platforms have commoditised these attacks, allowing even unskilled criminals to launch sophisticated campaigns. Abnormal Security reported a **30% year-over-year rise in phishing across the APAC region, confirming this is a regional trend.**

Most concerning, research shows that AI-generated phishing emails can match the effectiveness of human-crafted attacks and are bypassing traditional detection tools more easily than previous generations of threats.

## Implications

The threat is evolving faster than traditional defences can adapt. Email gateways and user awareness training are proving insufficient against AI-generated, highly personalised phishing attacks.

The shift to digital channels creates an opportunity: these channels generate data that can be analysed systematically, making them amenable to automated detection. However, nearly half of all scam reports and financial losses come from individuals aged 55 and above, suggesting that interventions targeting this demographic could have higher positive impact.

## Recommendations

**Phishing** should be the primary focus for intervention efforts. Its high volume, c**onsistent growth, and digital channel concentration make it both the most urgent threat** and the most feasible to address through technological means.

An effective solution must:

- **Operate across email and text message channels** where phishing now occurs most frequently
- **Analyse message content, context, and sender behaviour patterns** at scale and in real-time
- **Be automated and scalable to handle** the volume of phishing attempts
- **Prioritise the 55+** demographic in solution design

Traditional defences should be maintained but cannot be relied upon as primary protection against AI-driven attacks.

# Next Step

Building on the insights from this analysis, the project will advance through the following phases:

- **Phase 2: Phishing Threat Landscape Research** - Conduct in-depth research into current phishing attack methodologies, emerging threats, and the specific characteristics of AI-generated phishing campaigns. This phase will establish technical requirements for an effective detection system.

- **Phase 3: Solution Landscape Analysis** - Evaluate existing phishing detection approaches, including traditional rule-based systems, machine learning models, and commercial solutions. Document the strengths, limitations, and gaps of current methods to inform solution design decisions.

- **Phase 4: AWS Solution Architecture Design** - Design a comprehensive AWS-based architecture for the AI-driven phishing detection system. This will include service selection, data flow diagrams, integration patterns, and system component specifications

.

- **Phase 5: Prototype Development** - Build a functional demonstration system using AWS services to validate the proposed architecture and showcase core phishing detection capabilities.

# References


- Australian Bureau of Statistics (ABS) (2025) National, state and territory population: March 2025. Available at: https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/mar-2025#data-downloads (Accessed: 1 November 2025).

- Bentley, T. (2025) Beyond Spam: The Rise of Sophisticated Phishing Attacks in Australia. Abnormal Security. Available at: https://abnormal.ai/blog/rise-of-sophisticated-phishing-attacks-in-australia (Accessed: 12 November 2025).

- Scamwatch (2025) Scam statistics. Australian Competition and Consumer Commission. Available at: https://www.scamwatch.gov.au/research-and-resources/scam-statistics (Accessed: 25 September 2025).

- Mitchell, S.(2025) Phishing attacks surge as criminals exploit trusted platforms in 2025. SecurityBrief Australia. Available at: https://securitybrief.com.au/story/phishing-attacks-surge-as-criminals-exploit-trusted-platforms-in-2025 (Accessed: 19 November 2025).

- Venngage (n.d.) Accessible color palette generator. Available at: https://venngage.com/tools/accessible-color-palette-generator (Accessed: 10 November 2025).