MSc Cybersecurity, Privacy and Trust

EXPLORING FACEBOOK'S ROLE IN CYBERCRIMES: PLATFORM FEATURES, TRUST SIGNALS AND REGULATORY GAPS IN IRELAND

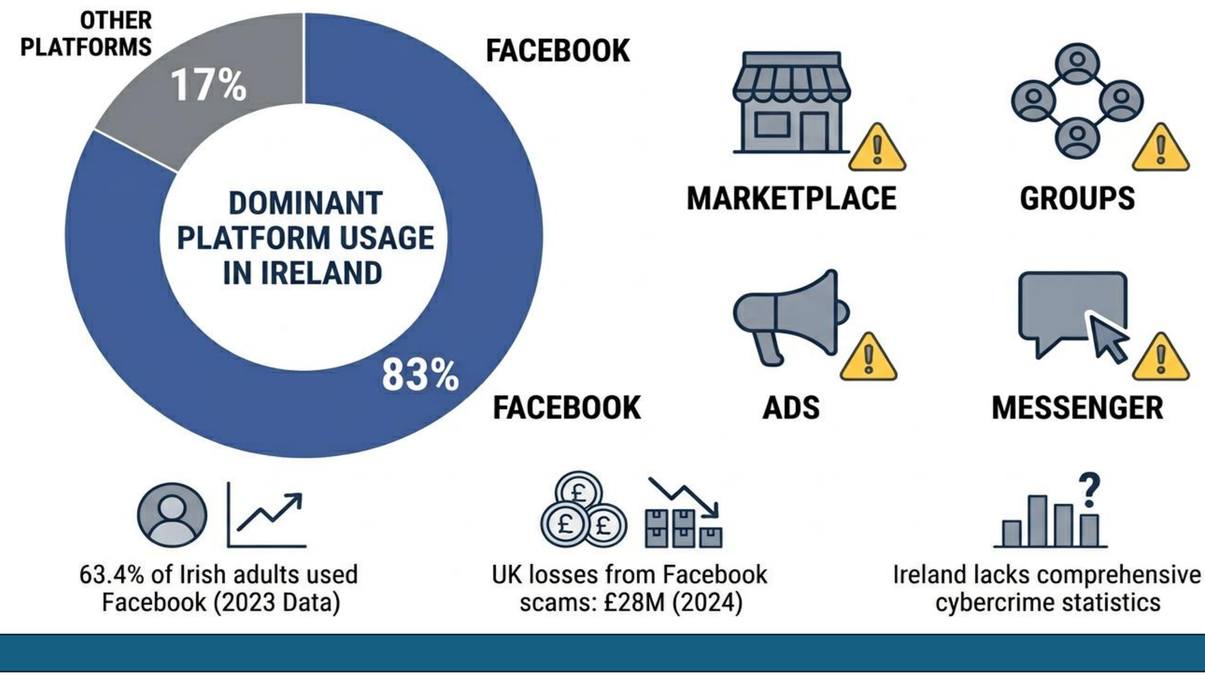
Julio Cesar Santana

Supervisor: Jamal Tauseef

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

INTRODUCTION

- Facebook holds 83% market share in Ireland (Statcounter, 2025)
- Used by 63.4% of Irish adults (DataReportal, 2025)
- Exploited features: Marketplace, Groups, Ads, Messenger
- UK losses from Facebook scams (2024): £28 million (Good Money, 2024)
- Ireland, however, lacks a comprehensive cybercrime statistics, with fragmented data across agencies and significant under-reporting of platform-enabled fraud (Gibbons, 2024).



RESEARCH QUESTIONS

1. Which Facebook platform features *(Marketplace, Groups, Ads, Messenger)* are exploited in reported scams in Ireland?

2. How do these features create trust signals or reduce friction in ways that may enable social engineering attacks?

3. How do current Irish and EU regulatory frameworks define and address platform responsibility for preventing fraud?

4. What gaps exist between regulatory requirements, platform transparency reporting, and documented scam patterns?

METHODOLOGY

- Approach: Qualitative case study + documentary analysis.
- Data sources: Meta transparency reports, Irish/EU regulatory texts (DSA, GDPR), scam reports, media coverage.
- Case selection criteria:
  - Relevance to Ireland
  - Clear fraud or social engineering
  - Involvement of Fake Profiles, Marketplace, Groups, Ads, or Messenger.
- Analysis: Thematic analysis + triangulation.

MOTIVATION / RESEARCH GAP

- Irish evidence gap: cybercrime data is fragmented and under-reported.
- Platform trust signals: badges, metrics, familiarity, and Marketplace features can be exploited.
- Policy gap: platform responsibility for fraud prevention remains unclear in practice.
- Previous research focuses mainly on users and attackers, leaving platform responsibility underexplored.

LITERATURE REVIEW

Prior research shows:

- Social engineering on social media exploits trust, urgency, and false authority.
- Facebook features such as feeds, badges, engagement metrics, and commerce tools can make fake content look legitimate.
- These design elements may create trust signals that increase willingness to share information or make payments.
- In Ireland, fragmented statistics and under-reporting make Facebook-enabled fraud difficult to measure.

EXPECTED OUTCOMES

- Identification of trust signals (e.g., verified badges, engagement metrics) that enable social engineering.
- Examine platform responsibility gaps and how features can contribute to fraud/scams.
- Highlight enforcement and transparency issues.
- Policy recommendations for platform design and regulatory reform in Ireland.

REFERENCES

AlAmeeri, A.A. and AlMourad, M.B. (2024). Impact of social engineering on social media users.
Chetioui, K. et al. (2022). Overview of social engineering attacks on social networks.
DataReportal (2025). Digital 2025: Ireland.
Gibbons, P. (2024). A quantitative analysis of cybercrime in Ireland.
Good Money (2024). The cost of Facebook scams in 2024.
Mezei, J. and Verteș-Olteanu, A. (2020). From Trust in the System to Trust in the Content.
National Cyber Security Centre (2025). 2025 National Cyber Risk Assessment.
Statcounter (2025). Social media stats Ireland.
Zhang, Y. et al. (2023). What do we mean when we talk about trust in social media?