CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Exploring romance fraud in an Australian context

Dr Cassandra Cross

Senior Research Fellow

Cybersecurity Cooperative Research Centre

Associate Professor

School of Justice

Queensland University of Technology

cybersecuritycrc.org.au

Today’s presentation

- Provides a summary of fraud with a focus on romance fraud
- Outlines the data used for the current project
- Explores how the military narrative is used by offenders in romance fraud
- Details how individuals respond to suspicions of inauthentic identities with those they communicate with
- Summarises the importance of the findings with some suggestions for future prevention messaging

Definition of fraud

- “The objective of fraud is to gain financial or other advantage over a person by means of deception” (Australian Bureau of Statistics, 2018)
- Various methods to perpetrate fraud, including both online and offline methods
- A financial advantage is usually gained through direct money transfers, but can also be through obtaining personal credentials

Categories of fraud

- There are endless "plot lines" that offenders can use to target victims (Cross and Kelly, 2016)
- Despite the variety, a consistent characteristic is a request for money or personal information
- Most common categories of fraud:
  - **Advanced fee fraud**: A person is asked to send a small amount of money in promise of a larger return (Ross and Smith, 2011)
  - **Romance fraud**: A person is defrauded under the guise of a legitimate relationship (Rege, 2009; Whitty and Buchanan, 2012)
  - **Business email compromise fraud**: Exploits established relationships through impersonation between business colleagues or trusted suppliers to gain a financial reward (Cross and Gillett, 2020)

Definition of romance fraud

- Instances where “criminals pretend to initiate a relationship via an online dating site or social networking site with the intention to defraud their victims” (Whitty, 2013: 666).
- Activities “where a person is defrauded by an offender/s through what the victim perceives to be a genuine relationship” (Cross et al., 2018: 1304).
- Can be initiated across a range of communication platforms
- Seeks to manipulate and exploit the desire of a person to connect with others through an intimate relationship

Fraud statistics 2019

- Billions is lost to fraud each year:
  - Australia - AUD$634 million (AUD$80 million)
  - USA - USD$3.5 billion (US$475 million)
  - UK - £1.2 billion (over £50 million in 2018)
  - Hong Kong – police intercepted HK$3 billion (US$385 million)
- These figures represent only a small proportion of actual losses globally
  - They do not incorporate a wide range of non-financial harms
  - Victims experience a decline in physical health, emotional well–being, relationship breakdown, unemployment, homelessness and in extreme cases, suicide (Button et al., 2009; Cross et al., 2016)
  - “Double hit” of victimisation (Whitty and Buchanan, 2012)

Techniques of offending

- Offenders use social engineering techniques
  - Authority, urgency, scarcity
- Offenders also appear to use psychological abuse tactics (established in domestic violence research)
  - Isolation, withdrawal, monopolisation

- The effective use of these facilitates victimisation of individuals

Why is fraud successful?

- Offenders are highly skilled, tech savvy individuals who know how to identify a person's vulnerability, to manipulate and exploit it
- Offenders can work in groups to target victims
- Offenders bombard victims with communications across all platforms
- Offenders always have an answer for any question which could potentially be plausible
- Victims do not believe that they are susceptible to fraud

The current data set

- Data on romance fraud reports was obtained from Scamwatch (online reporting portal for fraud hosted by the Australian Competition and Consumer Commission)
- Data was provided for the period July 2018- July 2019 (inclusive)
  - 4,358 reports filed during this time, with 3,463 (80%) able to be shared
- Each report included the following information:
  - Demographic details of the complainant (gender, age, and jurisdiction both within Australia and overseas),
  - Details about the fraud (how the approach was received, the location of the alleged offender), and any losses incurred (amount, payment methods, sensitive details lost).
  - Vulnerability indicators including age, disability, sickness, financial hardship, and location.
  - The de-identified free text field where each complainant wrote a summary/description of what happened.
- Upon review of the data, 204 duplicate entries were removed, leaving a final total of 3,259 distinct reports available for analysis.

Bryan Denny

- US retired army colonel who has had his identity stolen and used by romance fraud offenders multiple times globally

  - https://www.facebook.com/abcnews.au/videos/393240078098650/

https://www.pinterest.com.au/pin/105482816260001800/

https://www.counteringcrime.org/team/bryan-denny

Reference

Cross, C. and Holt, T. (2021) The use of military profiles in romance fraud schemes. *Victims and Offenders* 16(3): 385-406. DOI: 10.1080/15564886.2020.1850582

The military narrative

- Anecdotal evidence suggests that offenders frequently use a military profile to attract potential victims.

- This paper examined the following research questions:

1. Who is targeted by romance fraud offenders using a military narrative?
2. Is this group different to other categories of fraud victims?
3. How is the military narrative used by offenders to defraud victims?
4. Is this the same and/or different to what is currently known about romance fraud and advance fee fraud (AFF)?

- 463 reports in the data indicated the use of a military narrative

Two distinct categories of narrative

- Military identity as incidental to romance fraud narrative (military identity used to attract partner, but not part of overall story or reason for money)

- These focused on needs similar to traditional advance fee fraud:
  - Consignments and inheritances
  - Health emergencies
  - Criminal justice emergencies
  - Family assistance

- There was also combinations of these categories across the communications

- She claimed to have 40 gold bars she got paid for her work with the UN and was now trying to get the gold bars out of the country to the US. She claimed that she needed a load ok 56K to pay for her gold license gold seals security costs and other local government related taxes (case 2583)

- He said he was due to retire and needed help to get a suitcase containing personal paperwork out of the country. He asked me to make several payments on average of 1 000 (case 1836)

- He surposedly [sic] had to have a back operation so I sent money to pay for it as he said he was unable to access his funds or his travel insurance provider (case 999)

- Right now he is supposedly in Barcelona Spain. He has been accused of being a spy/terrorist. If I send his lawyer 2 000.00 he can get him out of jail and he can fly here to be with me (case 2375)

Two distinct categories of narrative

- Military identity integrated into both the overall story and the justification for financial requests
- These focused primarily on the following:
  - Leave requests (encompassing recreational/ retirement/ safety)
  - Supplies (food/ medicine/ phone/ internet)
- The justification for not being able to access funds was heavily focused on security and an inability while on deployment, to access their own personal funds.
- Security also provided a cover against communicating in an authentic way

- She said she will apply for a special exit to leave the army to move to Australia to be with me. She said it will cost a bit of money and could I support her. She asked if I could make a payment directly to the US Embassy (case 1094)

- He said he is with the US military and in Afghanistan. He wanted to get out of Afghanistan before he & his men get sent to Pakistan on a War zone. He's asked me to write email to [redacted] asking permission to come to Australia to marry me. I've got a reply from the email above asking me for money to pay airfare for [redacted]. I message [redacted] saying I can't send cash but I'm willing to pay his airfare using my credit card. [redacted] said that I need to send cash to U.N and they are buying his airfare. No I said. He then said that I'm allowing him to go to Pakistan to die (case 63)

- We talked for months as a good friend then suddenly again no communication because she got sick and she was asking money for toiletries (case 1128)

- He asked me if I could help him pay for his internet that the Army was going to turn him off (Case 408)

- In one week [he] started to be asking for money because as he said “According to the protocol from the start they didn’t let them have access to their banking account in need of some money and pay you back as soon as he gets home” (case 1064)

- He always refused video call or call, say[s] that it is forbidden for a soldier to make contact during their duty. And he mentioned that he used the military device to contact me with a consequences loosing [sic] of his job (case 80)

- He is claiming he is in army or National Guard in Afghanistan. He will tell u [sic] he is covert and can’t speak that he is on duty (case 2794)

Reference

Cross, C. and Layt, R. (2021) “I suspect that the pictures are stolen”: Romance fraud, identity crime and responding to suspicions of inauthentic identities. *Social Science Computer Review*. Online First DOI: 10.1177/0894439321999311.

Inauthentic identities & romance fraud

- Unsurprisingly, offenders do not use their own genuine identities. Those corresponding with offenders are often faced with situations where they question the identity of their partner.

- This paper explored the following research questions:
  1. What actions do individuals take in response to suspicions of inauthentic identities?
  2. How can this knowledge be used to improve future prevention messaging?

- 509 reports contained details in the free text related to the possible inauthenticity of the person they were communicating with

Verifying or mitigating suspicions

- When confronted with the possibility that the person may not be authentic, complainants detailed two courses of action:
  - Internet search
  - Third party assistance

- Internet searches could be successful in confirming suspicions
  - Stolen photos, facts not checking out, scammer websites

- The lack of evidence did not always affirm an identity
  - A lack of a digital footprint was seen to be suspicious in and of itself

- Third parties were asked to investigate facts and included family, friends and/or organisations

- I did a google search on his photo comes up heaps of times with different names and countries. (Case 2064)
- And the same day I checked his photo for scammers. HE IS THERE. (Case 3159)
- They then send a copy of the passport as “proof” and it is all wrong. I google the serial number for the passport and it is reported as fake. (Case 737)
- I have searched Facebook and google but can’t find any information on him anywhere—eg like he doesn’t exist in the real world. (Case 3292)

- My daughter helped show me the sight [sic] that can show of [sic] a picture has been edited and the first one we downloaded was the one where his head was slotted over the top of someone else's and that was when it hit me the total betrayal of this man. (Case 3379)

- I got suspicious and investigated from my end with [organisation] who emailed confirming that he does not work for them and they never need to ask for money when volunteering. (Case 104)

- I engaged an American investigator to find this person and they concluded that this person's address, phone number, personal details and email addresses were all fake. (Case 2793)

Conclusion

- Romance fraud is a significant problem that affects millions globally
- Financial and non-financial losses can be debilitating
- Current analyses provide some unique insights into romance fraud, across both victimisation and offending aspects
- Findings provide important lessons to improve prevention messaging

Contact

Associate Professor Cassandra Cross

Email: ca.cross@qut.edu.au

Twitter: @DrCassCross

Publications: http://staff.qut.edu.au/staff/raymentc/

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Cyber Security Research Centre Limited
ABN 11 605 454 144

cybersecuritycrc.org.au

Edith Cowan University
270 Joondalup Drive,
Joondalup WA 6027