

The Contacting of Adolescents on Social Media by Suspicious Accounts

Somaya AlWejdani
Richard Wortley
Jyoti Belur



THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato



Te Puna Haumarū
New Zealand Institute for
Security and Crime Science
THE UNIVERSITY OF WAIKATO

OUTLINE

Background



```
graph TD; A[Background] --> B[Aims]; B --> C[Method]; C --> D[Results]; D --> E[Conclusion];
```

Aims

Method

Results

Conclusion

BACKGROUND

Online Social Networks are the most common platform for online child sexual exploitation



Two sources of risk

Behaviour of users

Features of the network

Risky behaviours – routine activities

Amount of time
spent online

Amount and type
of personal
information
shared

Accounts and
websites
followed

Lack of parental
guardianship

Risky networks – lack of digital guardianship

Perfect ecology
for sexual
victimisation

Lack of
verification of
personal
information

Flags only when
seriousness
escalates

Algorithms may
connect minors
with suspicious
accounts

Honeypot designs

Honeypots: fictitious websites or user accounts used as bait to attract potentially malicious visitors



Most research self report, cross sectional – one previous ‘exploratory’ honeypot study



Advantages of honeypots

Don't rely on memory or honesty

Actual behaviour in real-life settings

Enable experiments

Participants self-selecting

AIMS

RQ1: How risky is the online social network environment for young users? Specifically, how likely are young users to be targeted by suspicious accounts?

RQ2: Does user profile information affect the online vulnerability of the user? Specifically, does the inclusion of a) a profile photograph and b) the absence of parental control, increase the likelihood of suspicious contacts?

RQ3: What role do online social network algorithms play in promoting suspicious contacts? Specifically, do online social networks suggest young users to follow suspicious accounts?

METHOD

Four fake profiles
of 13-year-old girls
on popular OSN

Mimicked real life
accounts

Posted generic
likes and follows

Follow similar
schedules

Responded to
innocuous
questions

Disengaged from
and reported any
sexualised
contact

Ran for 2 months

All accounts
contacting the
fake accounts
scrutinised

2 x 2 Design

Image

Oversight

Amy Graig



“My account is managed by my mum”

Chloe Daniel



“My account is managed by my mum”

Lisa Gordon



(No message)

Alice Andrew



(No message)

Defining suspicious accounts

Is the account holder an adult?

```
graph TD; A[Is the account holder an adult?] --> B[Does the account holder have a history of following children?]; B --> C[Does the account contain or send harmful or illegal content (HIC)?]; C --> D[Does the account holder engage in flirtatious, sexual, or otherwise inappropriate interaction with the fictitious account.];
```

Does the account holder have a history of following children?

Does the account contain or send harmful or illegal content (HIC)?

Does the account holder engage in flirtatious, sexual, or otherwise inappropriate interaction with the fictitious account.

RESULTS

	All	Types of Incoming activity				
		Like	Friend	Message	Video	Comment
Benign	67	37	29	1	0	0
Suspicious	201	53	87	47	11	3
Total	268	90	116	48	11	3

	Benign	Suspicious
Alice: No photo/No guardian	15%	10%
Chloe: No photo/Guardian	24%	15%
Lisa: Photo/No guardian	39%	52%
Amy: Photo/Guardian	22%	24%

Benign V Suspicious Accounts

		Benign N=47	Suspicious N=89
Apparent gender:			
	Female	26%	9%
	Male	46%	62%
	Unknown	28%	20%
Estimated age:			
	<20	51%	14%
	>20	32%	58%
	Unknown	17%	28%
HIC content:			
	No	96%	43
	Yes	4%	46
Following other children:			
	No	75%	9%
	Yes	26%	90%

Examples of Suspicious Accounts

Case 1: Adult, inappropriate messages

The account holder was an adult male. Most of his followed accounts were those of adult women and none were of children. He started a private chat thread with Lisa Gordon repeatedly asking about personal information, e.g., age, school, gender, family, mobile number. He repeatedly requested to connect via video calls, multiple times during a single day. A large proportion of the messages received were flirtatious although he never shared any HIC.

Case2: Following children, HIC content, inappropriate messages

The individual claimed to be a 17-year-old male, but photos suggested he may be an adult. He followed 1,227 accounts, including those of children. He initiated contact with Lisa Gordon and sent messages on a daily basis, including multiple video call requests. Messages received included inquiries about school, age, mobile number, and location. He regularly shared flirtatious content in the form of images, e.g., two people kissing or hugging. A phallic photo was received from him on the second day after initiating a connection with the fictitious account.

Case 3: Adult, following children, HIC content, inappropriate messages

An adult male who claimed to be a recruiter for a video gaming team. He followed 2,800 accounts, including those of children. He initiated a chat thread with Lisa Gordon right after his request to connect was accepted. He immediately initiated a private chat thread and shared messages of flirtatious content, e.g., “you are pretty”. Three days later, he shared a phallic photo with the fictitious account, and continued to follow up with questions such as “did you like it?”.

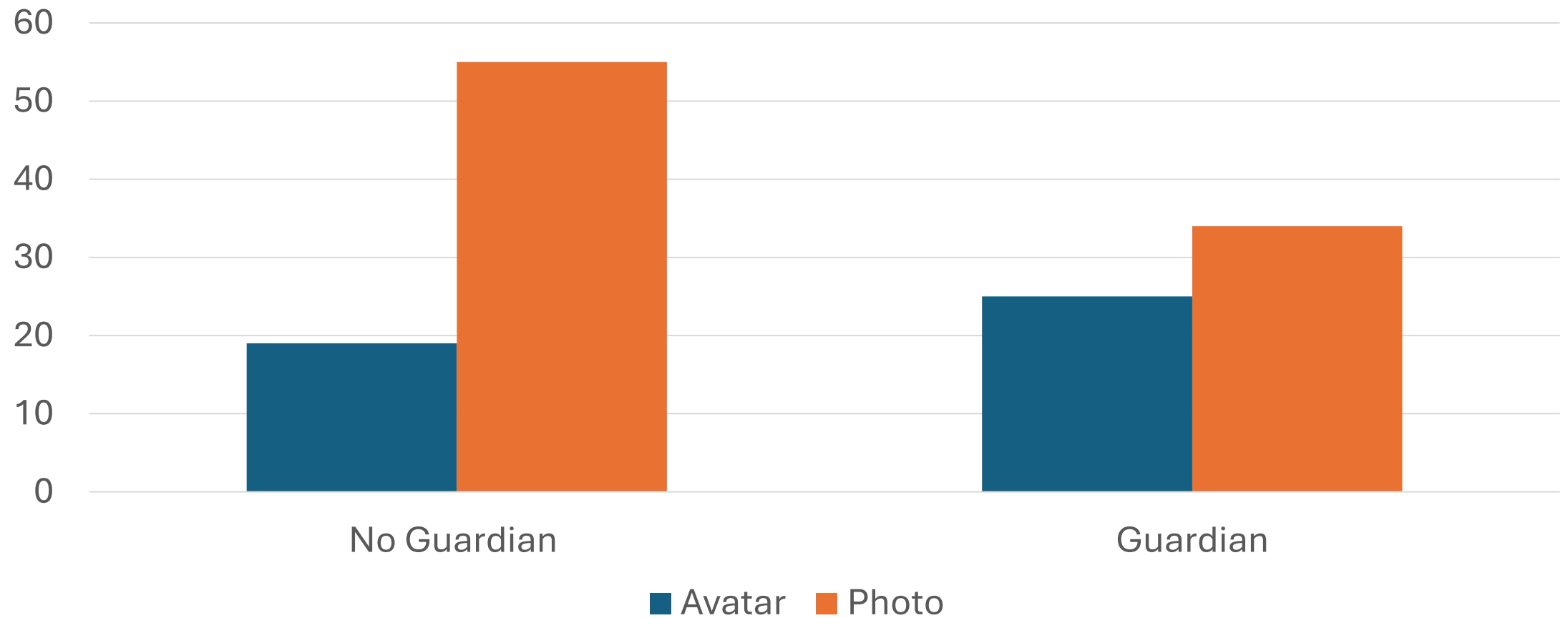
Accounts Contacting Fictitious Accounts

Accounts Chi-Square

Photo V Avatar	$X^2(1)=14.56, p<.001$
Guardian V No Guardian	$X^2(1)=1.48, p=.224$
Photo X Guardian	$X^2(1) =4.13, p=.042$
Fictitious X Ben/Susp	$X^2(3)=.921, p=.820$

	Benign N=45	Suspicious N=88
Alice: No photo/No guardian	13%	15%
Chloe: No photo/Guardian	16%	21%
Lisa: Photo/No guardian	47%	39%
Amy: Photo/Guardian	24%	26%

Interaction Image X Guardianship



Reason Given for Suggested Accounts

Reason X Ben/Susp $X^2(2) = 17.32, p < 0.001$

	Benign N=88	Suspicious N=32	Total N=120
Mutual friends	59%	28%	51%
New to OSNX	28%	25%	28%
OSNX recommendation	13%	47%	22%

CONCLUSION

RQ1: Around two thirds of contacts were from suspicious accounts

RQ2: Photo increases contacts, especially when paired with lack of parental oversight, but equally salient for benign and suspicious

RQ3: OSN algorithms can actively connect suspicious accounts with minors

Strengths, limitations, & implications

Honeypots a useful and underused research strategy

An account focus provides an opportunity for early detection

We cannot say for certain all suspicious accounts intent on sexual grooming

Need for age verification and limits placed on minors' accounts

Self protection strategies need to be accompanied by tighter network screening

How will AI and E2EE change the landscape?

