AUSTRALASIAN
CONSUMER FRAUD
TASKFORCE

AN INITIATIVE OF THE STATE, TERRITORY AND
AUSTRALIAN AND NEW ZEALAND GOVERNMENTS

Australian Government
Australian Institute of Criminology

Nigerian Scams

6th Joint London Action Plan

Contact Network of Spam Authorities Workshop

Dr Russell G Smith
Principal Criminologist
Russell.Smith@aic.gov.au

Melbourne, 20 October 2010

Understanding Nigerian scams

Origins in Australia

- Inspector John Nugent's *Registry of Flash Men*
- Fraudsters operating in Sydney 1841-44

Mick Bell

- "*one of the most cool, impudent vagabonds in Sydney*"
- Obtained money and clothes from Mr Monies on account to finance the smuggling of £20,000 worth of goods on a phantom ship in Port Hacking, out of the colony
- Mr Monies eventually realised that the scheme was fraudulent and reported the matter to the police
- Bell was convicted and sentenced to two months' imprisonment

Western Australia – April 2010

- WA woman offered to sell a $250 PlayStation on eBay in April 2010
- A bogus buyer made an offer, but asked for the item to be shipped to Nigeria

Understanding Nigerian scams

Fictitious funds transfer

- The woman received a fraudulent email from PayPal to confirm the transfer, and was then asked to pay additional shipping costs and duty
- Fraudulent Nigerian Customs forms and PayPal emails were then sent to confirm that payment had been made

Reported

- Suspecting a scam, the woman contacted WA ScamNet and was advised to break off all contact with the fraudsters
- After forwarding this email to the scammers, they sent false emails using the ScamNet logo, advising her to co-operate with the Nigerians
- She then received a fraudulent eBay email saying that the case had been reported to the Nigerian police, who had arrested the fraudster

Compensation

- A fraudulent police email told her that the Nigerian President had awarded her $US250,000 ($A279,485) in compensation

Understanding Nigerian scams

Further claims

- A false document from the Nigerian Central Bank said that the woman had to pay a transfer fee of about $US7,000 ($A7,800) before the money could be released
- She replied that she couldn't afford to pay as she was a single parent, and the scammers told her to take out a loan

Final loss

- After paying about A$8,700, the woman went to WA ScamNet offices in Perth and was told that she'd been defrauded

Nigerian scam typologies

- Advance-fee strategies – black money, confiscated and stolen funds, inheritances, lotteries, car sales etc.
- Money laundering
- Personal information harvesting – for use in identity scams
- Extortion and kidnapping

Criminogenic environment

The Nigerian social context

- 152 million people
- 30 internal states
- British colony in 1861
- Independence in October 1960
- Corruption Perception Index 2.5
- Theft of oil and gas income
- Civil unrest & poverty from 1980s during General Abacha's regime
- Increasing stability since 2000 – *Bank CEO imprisoned October 2010*

A technology-enabled crime

- 2 billion global Internet users 30 June 2010 – 29% of world population
- 17 million Australian Internet users – 80% of Australian population
- 44 million Nigerian Internet users – 29% of Nigerian population (22,000% increase in Nigerian Internet users between 2000 and 2010)

ABS Personal Fraud Survey 2008

Sample

- 14,320 individuals, 15 years or older interviewed
- Asked about experiences during July to December 2007

Exposure to scams *(received, viewed or read invitations)*

- 35.8% exposed to scams (5,809,100 Australians)

Victimisation *(supplying information or money)*

- Victims of: identity fraud 3.1% (499,500); scams 2.0% (329,000)
- Lotteries (0.5%), pyramid schemes (0.4%), phishing and related scams (0.4%), financial advice (0.2%), chain letters (0.2%), other (0.4%), **advance fee fraud [16,000 Australian victims] (0.1%)**

Financial loss *(Money supplied without recovery)*

- 453,100 Australians lost money (2.8%)
- Total losses $977 million
- Mean losses $2,156 per person

ACFT / AIC online survey 2010

AUSTRALASIAN CONSUMER FRAUD TASKFORCE

AN INITIATIVE OF THE STATE, TERRITORY AND AUSTRALIAN AND NEW ZEALAND GOVERNMENTS

Methods

- Online questionnaire hosted by AIC – 1 January to 31 March annually
- Self-selected respondents with access to Internet
- Promoted during annual ACFT awareness campaigns

Questions

- Demographics – age, gender, region and income
- Scam invitations – type, method received, number received
- Victimisation – financial and other loss
- Reasons for *not* responding to a scam invitation
- Reporting behaviour, and perceptions of legality or otherwise

Sample

- 2008 survey – 919 respondents
- 2009 survey – 692 respondents
- 2010 survey – 248 respondents

AUSTRALASIAN CONSUMER FRAUD TASKFORCE

AN INITIATIVE OF THE STATE, TERRITORY AND AUSTRALIAN AND NEW ZEALAND GOVERNMENTS

Online Survey Results 2008 & 2010

Scam type	Invitation received 2008 (%)	Responded positively 2008 (%)	Invitation received 2010 (%)	Responded positively 2010 (%)
Lotteries	55	6	56	5
Phishing	54	4	50	3
Advance fee fraud	**53**	**5**	**52**	**3**
Financial advice	35	4	26	2
Other (dating, wills, jobs)	33	10	61	9
Any type of scam	90	18	89	29

n=919 (2008); n=248 (2010)

Australian Government
Australian Institute of Criminology

Source: AIC online survey computer file

Online survey results 2010

Victimisation

- 59% who responded provided personal details / passwords (n=25)
- 36% who responded provided money – total losses $750,074
- Range of funds sent – $92 to $614,200; mean $28,849
- 14% of advance fee responders sent personal details (n=6, p<=0.01)
- 11% of advance fee responders sent money (n=3, p<=0.05)
- 77% of advance fee responders identified it as a ‘crime’

Scam types – receipt and responses

- Phishing most commonly received (51%) – lowest response rate (5%)
- Dating least likely to be received (18%) – highest response rate (27%)

Mode of receipt

- Most received via email (85% of email receipts were advance fee)

Reporting

- 55% of advance fee scam recipients reported to Police, Consumer Affairs or AFP High Tech Crime Operations

Online survey results 2010 by age category

Younger age category (under 25 years – 33%)

- Significantly less likely to receive any invitation (n=21, 66%, p<=0.01)
- Significantly likely to respond to advance fee frauds (n=3, 30%, p<=0.01), inheritance scams (n=1, 20%), phishing scams (n=2, 18.2%) and financial scams (n=1, 14.3%)
- Received scams via SMS more than any other age group (28%, p<=0.01); received Internet scams more than any other age group (16%)

Middle age category (25 to 54 years – 32%)

- Middle and older age groups were more confident in detecting a scam than younger people (82%, p<=0.01)
- Middle age group most likely to respond to lottery scams (n=7, 8.8%) and dating scams (n=9, 34.6%)

Older age category (55 years and older – 31%)

- Significantly more likely to receive lottery scams (71%, p<=0.01)
- Most likely to respond to job scams (n=4, 12.1%)

(n = 217 who provided information on age)

Why people respond to scams

Routine activities theory *(Cohen & Felson 1979)*

- Opportunities, motivated offenders, absence of capable guardians
- High internet usage with lax security measures enhances risk

Life-style exposure theory *(Hindelang, Gottfredson & Garofalo 1978)*

- Demographic variables in conjunction with lifestyle relate to risk
- Age, sex, education and income level may be correlated with risk levels
- Negative life events may increase vulnerabilities through a desire to respond to grief or loss by engaging in consumerism or risk-taking

Self-control theory *(Gottfredson & Hirschi 1990)*

- Low self-control and impulsiveness may enhance vulnerabilities
- Desire for immediate gratification increases risk
- Participating in financial risk-taking enhances risk
- Responding to scams without undertaking checks creates risk

AIC/UniMelb/VicPol advance fee fraud study 2008

Aims

- Using a sample of individuals who had transferred funds to Nigeria, to determine the extent to which the funds transfers involved scams, and the risk factors and reasons why funds were sent

Population

- 9,241 Victorians transferred funds to Nigeria using Western Union from 1 April 2007 to 31 March 2008 (12 months) – Victoria Police data
- 7,831 excluded (multiple transactions, non-Victorian, incomplete address information, multiple individuals at one address)

Sample / results

- 1,410 individuals sent questionnaire by 3 September 2008
- 202 responded (14%); 120 victims (59%); 82 non-victims (41%)
- Total funds sent ranged from $100 to $120,000; mean approx. $12,000
- Other advance fee (33%), dating (36%), financial assistance (11%), online transactions (9%), lotteries (8%), job offers (7%)

Significant risk factors (those more likely to be victims)

Demographics

- Older age groups (45-54, >65); Lower income groups (<$20,000 pa)
- Lower education (secondary schooling or lower); Unemployed

Lifestyle

- Suffered from depression in last five years
- Suffered a personal financial crisis or lost job in last 5 years
- Diagnosed with a serious illness in last five years

Risk-taking

- Likely to trust strangers; Likely to make impulsive decisions
- Unlikely to wait for something due

Computer usage and security

- Likely to use the Internet for longer hours (10-19, >20 hours a week)
- Likely to employ more computer security measures

Response strategies

Continuing research to improve evidence base

- Further qualitative research on high risk groups

Targeted fraud awareness and risk reduction information

- Older age groups, lower income groups, less educated, unemployed
- Information for those with mental health problems or serious illnesses
- Information for those likely to be risk-takers

Solutions directed at computer users

- Enhanced training of users to maintain computers adequately
- Enhanced training of users to avoid risky behaviours
- Software solutions to make high risk behaviour impossible
- Enhanced security of personal information online

Enforcement and disruption

- Transaction monitoring, notification, advice and blocking
- Targeted law enforcement action

Australian Government
Australian Institute of Criminology

Russell.Smith@aic.gov.au