Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 706

Developing a harm index for individual victims of cybercrime

Appendix

Isabella Voce and Anthony Morgan

Table A1: Cybercrime categories used in the development of the harm index

	n
Online shopping scams	**115**
I paid money or provided sensitive information to a fake seller or buyer online	104
I paid money for health products, medicines or drugs from an online pharmacy and the products never arrived or were counterfeit	14
Investment and betting scams	**19**
I paid money or provided sensitive information to a scammer to buy into an illegitimate investment, trading or shares scheme or to get early access to my super fund	2
I lost cryptocurrency to a scammer in a pretend 'give away', business opportunity or investment opportunity	6
I lost cryptocurrency in an exit scam or rug-pull—where cryptocurrency developers or promoters abandon a project and disappear with investors' funds	10
I lost money buying sports betting prediction software, or becoming the member of a sport betting syndicate or investment scheme because these schemes did not work as advertised	2
Remote access scams	**24**
I allowed someone pretending to be a telecommunications or computer company to remote access my computer, or paid them money or provided sensitive information	24

Table A1: Cybercrime categories used in the development of the harm index (cont.)	
	n
Phishing scams	**65**
I paid money or provided sensitive information to a scam falsely offering a rebate from the government, a bank or trusted organisation	4
I paid money or provided sensitive information to a scammer pretending to be a charity or disaster relief effort	2
I lost money or provided sensitive information to a scammer offering a job or employment	6
I provided sensitive information to a scammer pretending to be a known service institution or company (bank, internet provider, post office, etc)	29
I paid money or provided sensitive information to someone pretending to be a bank, government or law enforcement official for things like a speeding fine, tax office debt, or immigration or visa issues	1
I paid a fake invoice for directory listings, advertising, domain name renewals or office supplies	0
I sent money to a scammer posing as a known business supplier, service institution or company telling me that their banking details have changed	12
I paid money or provided sensitive information to a scam offering me the false promise of an inheritance or share in a large sum of money in exchange for my assistance	3
I paid money or provided sensitive information to a scam offering the false promise of prize money or a holiday package	6
I paid extremely high call or text rates when replying to unsolicited SMS competitions	1
Extortion or harassment involving images or videos	**119**
I was threatened with the release of sensitive, personal, compromising or intimate photos, video or information that was stored online, on a digital device or sent in messages	96
Someone used coercion, blackmail or demands to try and get me to send them sensitive, personal or compromising photos, video or information that was stored online, on a digital device or sent in messages	17
Someone sent or posted photos and videos of me to others to try and embarrass, hurt or blackmail me	8
Doxxing	**36**
Someone published identifying information (such as my full name, contact number, address, school etc) with malicious intent (ie doxxing)	36
Impersonation	**235**
Someone hacked into my social media or network account (including communicating with my contacts or posting messages or status updates from my accounts)	152
Someone set up fake social media or networking profiles pretending to be me (eg and communicated with my contacts or posted messages or status updates from my accounts)	87
Someone created fake videos or photos of me (eg 'deep fakes')	7

Table A1: Cybercrime categories used in the development of the harm index (cont.)	
	n
Stealing or sharing content without consent	**51**
Someone shared or published sensitive, personal, compromising or intimate photos or videos of me without my consent	16
Someone stole my online personal information (including photos and videos) and used it without my permission	36
Stalking and harassing	**45**
Someone used technology to stalk or repeatedly harass me, including being contacted by someone I have blocked or asked to not contact me	45
Controlling and restricting behaviour	**88**
Someone tried to stop me from communicating with others online or over my mobile	25
Someone restricted my access to online resources (eg social media, electronic legal documents, banking and utility accounts, etc)	45
Someone monitored my activity online or on my phone (including installing spyware, going through my private messages, etc)	27
Hate speech	**46**
Someone subjected me to hate speech or made derogatory, malicious or threatening comments directly to me based on my religion, ethnicity, gender, sexuality or ideology	46
Cyberbullying	**122**
Someone sent or posted mean or hurtful messages via electronic communication (eg emails, social media or text messages) that made me feel hurt, embarrassed or unsafe	100
Someone spread rumours about me via electronic communication (eg emails, social media or text messages)	28
Unsolicited sexual content	**489**
I was sent unsolicited sexually explicit messages, images or videos	489
Compromise of financial accounts	**914**
Someone tried to obtain money from one of my investments or superannuation accounts	16
Someone tried to open a new bank account, apply for a new loan or obtain credit with my personal information or I received credit/payment cards in the mail that I did not apply for	22
I was unsuccessful in applying for credit, and this was surprising given my credit history	22
Someone used my personal information to purchase or order something or I received unfamiliar bills, invoices or receipts	93
I received calls from debt collectors asking about unpaid bills I didn't recognise	280
Suspicious transactions appeared in my bank statements or accounts, credit card or credit report	562

Table A1: Cybercrime categories used in the development of the harm index (cont.)	
	n
Other identity compromise	**32**
Someone gained access to my cryptocurrency wallet or exchange account and made transactions or stole currency	2
Someone used my personal information to create a fake cryptocurrency wallet or exchange account	3
Someone used my personal information to fraudulently apply for government benefits	1
I was unable to file taxes because someone had already filed a tax return in my name	3
Someone used my personal information (including images) to create an impersonation account to extort my contacts	9
Someone used my personal information to open up a mobile phone or utility account, or my current mobile phone or other utility lost service because my service has been transferred to a new unknown device	11
I got a medical bill for a service I didn't receive, or my medical claim was rejected because I had unexpectedly already reached my benefits limit	6
Someone used my personal information to attempt to apply for a job or rent a property	1
Someone used my personal information to attempt to give false info to police	2
Ransomware	**20**
My devices, servers, service or networks were disrupted (eg slowed down, lost connection, had outages) and I received instructions for paying a ransom to restore functionality	11
My systems, devices or files had a virus or were inaccessible (eg locked or unreadable) and I received instructions for paying a ransom to restore access	9
Data theft and extortion	**83**
I received a ransom message on my device to say my data or information had been stolen and I had to pay to prevent this information from being leaked or sold online	83
Other malware	**802**
Pop-up ads started popping up everywhere	226
My device slowed down and acted strangely	297
People I knew told me I had been sending suspicious messages and links over social media or email	72
My devices kept crashing for some reason	10
My browser kept getting redirected when I tried to search for a familiar site	112
My device was working excessively while no programs were running	57
There was a lack of storage space that I couldn't explain	69
Programs were opening and closing automatically	79
Previously accessible system tools (such as personalised or security settings) were disabled	117
My files had gone missing or been replaced with odd file extensions and the icons for the files were blank	6

Isabella Voce is a Principal Research Analyst in the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.

Anthony Morgan is Research Manager of the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.