Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 680

Abstract | The rise of the internet or, more specifically, of services offered and conducted online has led to a dramatic rise in frauds and scams. This study is a systematic review of the literature on the use of crime script analysis in the field of fraud facilitated by the internet to identify stages of the crime commission process across different forms of fraud and examine ways to disrupt those crimes. The scripts for different forms of fraud shared three common elements: communicating with the victim, recruiting enablers, and using money mules. These common elements suggest possible prevention measures. Future applications of crime scripts in the field of fraud and financial crime more broadly are discussed.

Examining emerging fraud facilitated by the internet through crime scripts

Benoit Leclerc and Elena Morgenthaler

Fraud potentially represents the broadest category of crime, including financial crimes such as lottery fraud, investment fraud and romance fraud. Arguably, the ultimate goal of any of these crimes is financial gain. Capturing all types of fraud alone is difficult and typologies have been developed in part for this reason (Levi 2008). The rise of the internet or, more specifically, of services offered and conducted online has led to a dramatic rise in frauds and scams (Emami, Smith & Jorna 2019). For instance, cyber-enabled fraud has become one of the most prevalent crimes globally (National Audit Office 2017). To illustrate, the UK National Audit Office (2017) indicated that, out of 11.8 million reported crimes in the United Kingdom in 2015–16, 3.6 million were fraud related, and of those 3.6 million, more than half (1.9 million) were cyber-related frauds.

The Internet Society's Online Trust Alliance (2019) estimated that the annual cost of cybercrime, including the cost of efforts to disrupt cybercrime internationally, reached US$45b in 2018. Consequently, it is no surprise that the global cybersecurity market is ever increasing as well. In 2021, this market had a value of US$184.93b and was expected to expand at a compound annual growth rate of 12 percent between 2022 and 2030 (Grand View Research 2023). The Grand View Research report indicates that this growth is partly explained by the increasing number of cyber attacks, the emergence of ecommerce platforms and the proliferation of smart devices, which is consistent with the situation in Australia.

As most business services are moving (or have already moved) online, a rise in frauds and scams is expected. Essentially, most types of fraud can be displaced and conducted online. Cyber-enabled fraud further includes crimes such as phishing emails, malware and identity theft carried out via a compromised email account—crimes linked to fraud or financial crimes. For instance, phishing emails appear to come from a trustworthy source but direct the recipient to the scammer's own website, which generally asks them to enter personal information such as passwords. Individually tailoring these emails to a specific recipient is known as 'spear phishing' (Broadhurst & Trivedi 2020). Broadhurst and Trivedi (2020) indicated that the Australian clearing house for fraud alerts received nearly 25,000 phishing scam reports in 2018 alone. The Australian Bureau of Statistics (2016) estimated that 1.6 million Australians experienced personal fraud in 2014–15, with losses for all personal fraud (including scams, credit card fraud and identity crime) reaching $3b (see Emami, Smith & Jorna 2019). The COVID-19 pandemic created further opportunities for numerous other types of financial misconduct and fraud to arise (Levi & Smith 2021).

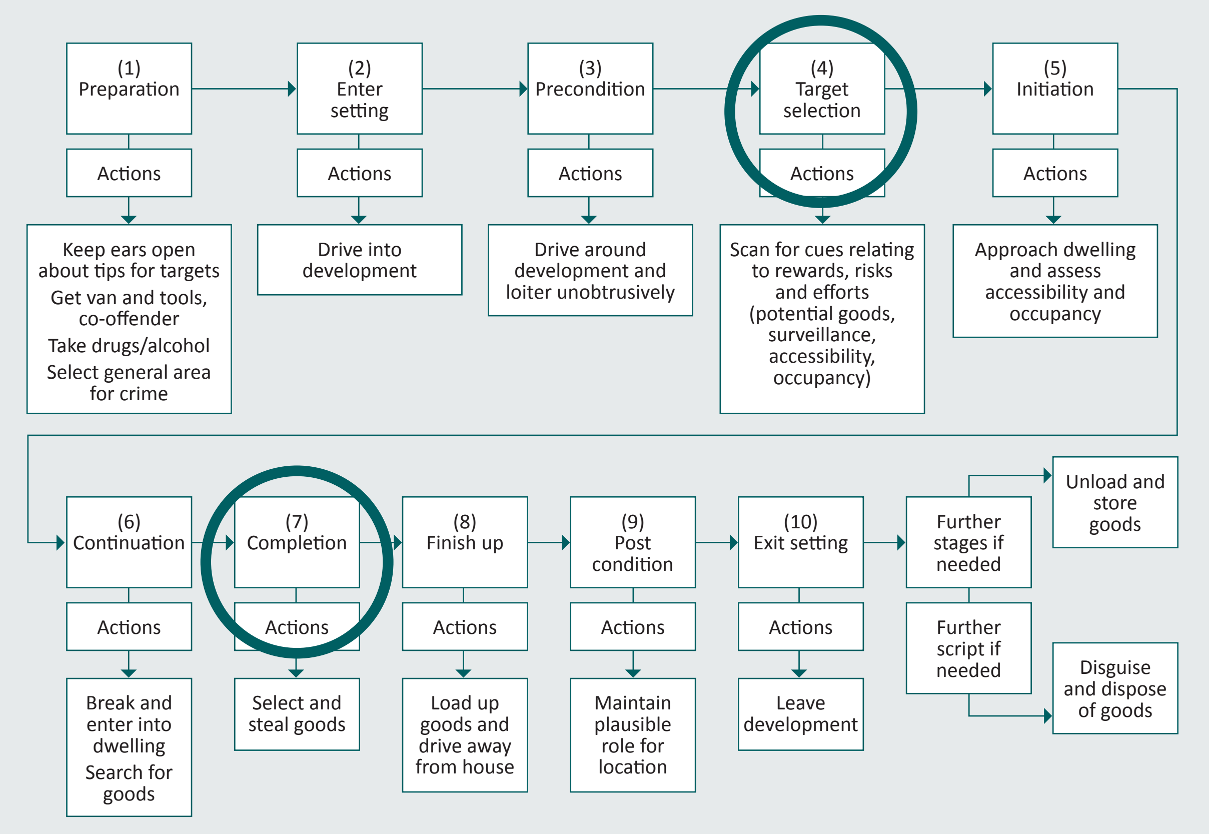
Evolving technologies have allowed offenders to target much larger pools of victims, operate with high levels of anonymity, and commit crime across borders while evading detection. While offenders continue to employ traditional financial fraud methods, they are increasingly using cyber environments to expand opportunities to offend (Lee & Holt 2020). For example, one self-managed super fund scam involved offenders both cold-calling consumers (a traditional offline scam method) and operating websites to recruit and engage with victims (Australian Securities and Investments Commission 2020). Several regulatory agencies have a mandate to address this crime type, including police agencies, the Australian Securities and Investments Commission and AUSTRAC. However, more capacity is needed to efficiently address this phenomenon (see, for example, Drew & Drew 2010; Lee & Holt 2020). Indeed, in response to the rise of cybercrime in Australia, the Australian Federal Police led Joint Policing Cybercrime Coordination Centre was launched in 2022 to enhance intelligence sharing, coordinate training and communicate nationally consistent prevention and awareness raising messages to industry and the public. In 2023, the Australian Competition and Consumer Commission (2023) was allocated $58m to establish the National Anti-Scam Centre, which will help build the technology needed to support data sharing between law enforcement and the private sector. Offenders adapt quickly to regulatory and legislative responses and are taking advantage of the enhanced criminal opportunities afforded by an online and interconnected world. To address this phenomenon more efficiently, it is critical that a wide and complementary range of initiatives and methodologies are established and used to identify how offenders operate and adapt to intervention initiatives.

In this study, we review the literature on crime script analysis in the field of fraud facilitated by the internet to identify stages of the crime commission process across different forms of fraud and suggest ways to disrupt those crimes. We also discuss future applications of crime scripts in the field of fraud and financial crime more broadly.

Crime script analysis

Crime script analysis emerged as a critical method to understand the operating processes of offenders for prevention purposes in the mid-90s (Cornish 1994). There are two key reasons for performing crime scripts. First, scripts offer a template to break down and identify the step-by-step process of crime commission. As an example, Figure 1 illustrates the crime script of a suburban burglary. Second, and most importantly, scripts generate new avenues to neutralise crime. Specifically, once mapped out, the script can be used to pinpoint different intervention solutions that could be applied at each step of the process, whether to improve investigation, monitoring, detection or prevention (see, for example, Leclerc 2014, 2016, 2017; Leclerc & Wortley 2013; Leclerc, Wortley & Smallbone 2011). The selection of steps can be made for strategic reasons—for example, if the offender has only one way to complete the step or if the step is critical to carrying out the crime. Figure 1 showcases that the target selection and the completion steps could be chosen to disrupt the crime. In addition, all steps can be used simultaneously as intervention points where possible and relevant.

Figure 1: Disrupting suburban burglary at the target selection and completion step

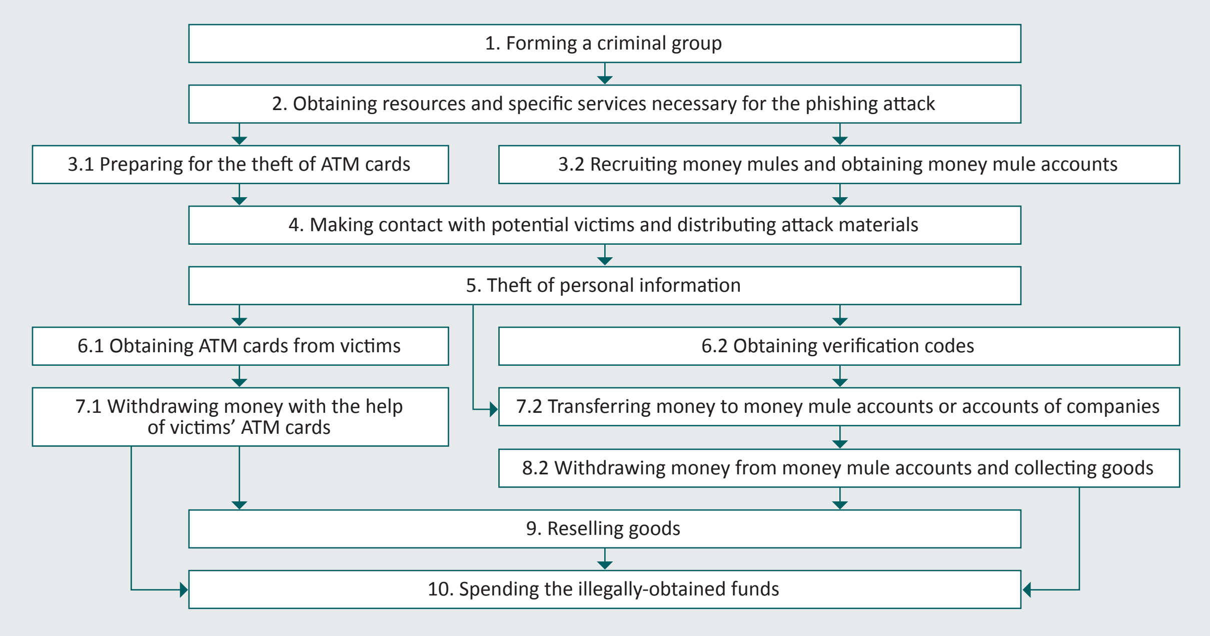

(1) Preparation
Actions
Keep ears open about tips for targets
Get van and tools, co-offender
Take drugs/alcohol
Select general area for crime
(2) Enter setting
Actions
Drive into development
(3) Precondition
Actions
Drive around development and loiter unobtrusively
(4) Target selection
Actions
Scan for cues relating to rewards, risks and efforts (potential goods, surveillance, accessibility, occupancy)
(5) Initiation
Actions
Approach dwelling and assess accessibility and occupancy
(6) Continuation
Actions
Break and enter into dwelling
Search for goods
(7) Completion
Actions
Select and steal goods
(8) Finish up
Actions
Load up goods and drive away from house
(9) Post condition
Actions
Maintain plausible role for location
(10) Exit setting
Actions
Leave development
Further stages if needed
Further script if needed
Unload and store goods
Disguise and dispose of goods

Source: Leclerc (2017)

Script analysis can be applied to complex criminal activities such as organised crime, in which different steps in the script are undertaken by different actors (Cornish & Clarke 2002). It is arguably the most efficient decision-making framework to identify how offenders operate. It identifies each step of the crime commission process, and this knowledge provides a template to generate crime-proofing solutions (Cornish 1994; Ekblom & Tilley 2000).

In relation to fraud, this approach should be used to gather insights into offenders' operational knowledge, which in turn can help to disrupt any fraud activity, online or offline. An example of a crime script applied to phishing attacks for financial gain from Loggen and Leukfeldt's (2022) study is provided. There are two variants to the script—one on the left-hand side (3.1, 6.1 and 7.1) and one on the right-hand side (3.2, 6.2, 7.2 and 8.2). The middle of the script represents steps common to both variants (Figure 2). This script is explained in detail in the *Results* section.

Figure 2: Crime script of a phishing attack


1. Forming a criminal group
2. Obtaining resources and specific services necessary for the phishing attack
3.1 Preparing for the theft of ATM cards
3.2 Recruiting money mules and obtaining money mule accounts
4. Making contact with potential victims and distributing attack materials
5. Theft of personal information
6.1 Obtaining ATM cards from victims
6.2 Obtaining verification codes
7.1 Withdrawing money with the help of victims' ATM cards
7.2 Transferring money to money mule accounts or accounts of companies
8.2 Withdrawing money from money mule accounts and collecting goods
9. Reselling goods
10. Spending the illegally-obtained funds

Source: Loggen & Leukfeldt 2022

Commonly paired with scripts is the situational crime prevention approach. Situational crime prevention is typically applied to implement measures to:

- increase the effort required and risk involved for individuals or groups to conduct criminal activities;
- reduce the rewards associated with committing crimes; and
- remove excuses that individuals may use to justify getting involved in these activities.

One core assumption of situational crime prevention is that crime increases when opportunities to offend emerge (Clarke 2008), which is perfectly consistent with the rapid emergence of fraud facilitated by the internet, financial crime and scams in Australia. Crime script analysis is not limited to situational crime prevention efforts—this approach can also be used to improve the investigation processes and detection strategies used by police and banks (Leclerc 2017; Leclerc et al. 2021) or to understand and improve the intervention processes used by the police or citizens (Leclerc & Reynald 2017).

Empirical research exploring specific aspects of fraud has increased in the past decade, potentially in part due to the role of the internet and advances in technology. To date, however, this body of knowledge has not been consolidated to provide a baseline perspective of what is known about different aspects of offending processes used by fraud offenders. The aim of the current study is to conduct a systematic review of the empirical literature on crime script analysis in the field of fraud facilitated by the internet. The first goal is to assess what is known from script analysis of the crime commission process involved in different forms of fraud. The second goal is to identify important stages of the crime commission process across different forms of fraud and examine possible ways to disrupt those crimes. Building on these two goals, the third goal is to look at future applications of crime scripts in the field of fraud and financial crime more broadly to help build the capacity of financial organisations to protect themselves and to inform policymakers.

Methods

Search strategy

To address the research question a search of relevant academic databases for current literature was conducted between November and December 2021. The search terms and databases used are listed in Table 1. Databases searched were Informit, ProQuest, Ovid, EBSCO and Web of Science. These databases have been previously used in a study by Cale and colleagues (2021). The broad term 'fraud' was used for searches to yield the greatest number of records. The search terms used for concept 2 were based on terms frequently used in research on crime scripts and offending behaviour. Different search terms were used for each database due to the large and unmanageable results yielded by some searches conducted. Searches resulting in more than 1,000 records were deemed too large to manage and not included. Most searches listed below resulted in fewer than 100 identified records. Additionally, only records published in or after 2008 and written in English were included.

Table 1: Search terms used

	Concept 1	Concept 2
Informit, ProQuest, Ovid, EBSCO, Web of Science	Fraud	Crime script Crime commission process
Informit, Ovid, EBSCO, Web of Science	Fraud	Modus operandi
Informit, Ovid, EBSCO	Fraud	Strategy Technique
Informit, EBSCO	Fraud	Commit

Inclusion and exclusion criteria and analytic method

The selection of records for this systematic review was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA; Moher et al. 2009). The initial searches returned 3,246 results. Five additional records were identified through citation chaining, bringing the total number of identified records to 3,251. Duplicates were identified and removed, which resulted in 1,970 records for screening. These were screened through manual examination of titles and abstracts, leading to the exclusion of 1,792 items. This was followed by screening the full texts of 178 items.

The main inclusion criterion used was the discussion of a crime script of cyber-enabled fraud or the behaviours adopted by offenders to engage in this type of crime. Documents that did not discuss any monetary transaction or strategies to commit fraud facilitated by the internet were excluded, as a financial transaction and a cyber element to the strategies used by offenders were a pre-requisite for inclusion in this review. Any records which focused only on technological aspects or accounting perspectives were also excluded. Documents in which the data source was not revealed (*n*=1) or that were based on literature reviews as opposed to empirical evidence (*n*=2) were excluded. This resulted in a total of 17 studies on crime scripts.

Finally, two additional studies were added to include the most recent studies in this field, leading to a total of 19 studies. Although not specifically fraud, the study on ransomware by Matthijsse, van't Hoff-de Goede and Leukfeldt (2023) was included because the ransomware was conducted by offenders for financial gain and the study applied crime script analysis to ransomware for the purpose of identifying prevention measures. It should also be noted that Loggen and Leukfeldt's (2022) study is an expansion of two other studies conducted by Soudijn and Zegers (2012) and Leukfeldt (2014).

Results

Nineteen studies specifically addressed the aims of this study. As seen in Table A1 (see *Appendix*), the types of fraud facilitated by the internet to which crime script analysis has been applied include phishing, smishing (phishing carried out via SMS messages), eWhoring (a type of online fraud in which cybersexual encounters are simulated for financial gain), ransomware, stolen data, carding (where a stolen credit card is used to charge prepaid cards online), phone scams, romance scams, and investment fraud. For instance, Choi and Lee (2021) used victims' narratives posted on South Korea's most popular websites (Naver, Daum, Google, YouTube) to apply crime scripts to smishing. The pre-crime phase included purchasing potential victims' personal information as well as preparing for the smishing attack by arranging, setting up and uploading a malicious application. The crime phase was characterised by sending the smishing message with a link to the website hosting the malicious application. When the victim clicks on the link, the malicious application is downloaded on the smartphone and the theft of personal information occurs. Each victim's information is then used for charging payments to the victim.

Leukfeldt (2014) examined a case study of one criminal organisation involved in phishing. Information obtained through phone taps and interviews with the investigation team was used to create the script. One of the first steps identified is to send emails to potential victims, appearing to be from the victim's bank, seeking information or asking them to click on a link leading them to a phishing website. To obtain the code needed to access the victim's account, the offender uses information obtained directly from the victim. The offender makes a telephone call posing as a bank employee and pretending that a new security measure requires the victim to share a unique code. Upon receiving the code, the offender transfers money from the victim's account to their own accounts.

Building on this earlier study, Loggen and Leukfeldt (2022) found more detailed insights into the methods and process of phishing. The script starts with the formation of a criminal group with core members, followed by the group gaining access to phishing websites and messages, forged documents and spam software that can be used to send large amounts of emails or text messages.

The offenders then steal ATM cards or recruit money mules, whose accounts they transfer money in and out of to disguise their own identities. Often money mules voluntarily give offenders their ATM cards for a commission, but in some cases they might be forced to. When the ATM card or personal information is obtained from the money mule, the offender's next steps include:

- contacting potential victims and distributing attack materials;
- stealing personal information; and
- obtaining ATM cards of victims or verification codes.

In most cases, the verification codes are obtained by calling the victim and pretending to be a bank employee. The next step involves withdrawing cash using the victim's ATM cards or transferring money to a money mule account. In the latter case, offenders often transfer the money themselves to money mules. The last steps generally include:

- withdrawing cash from the mule accounts directly from ATMs;
- reselling goods such as cars that were bought with the money; and
- spending the money on goods where cash has been withdrawn or where goods have been resold for cash.

Another example of a crime script is presented by Hutchings and Holt (2015). Using 13 stolen data market forums, Hutchings and Holt (2015) identified several important steps across the crime commission process involving offenders (buyers and vendors), starting with the preparation of the crime. This involves setting up the necessary software, creating accounts, ensuring anonymity and security, locating a marketplace as well as learning specialist knowledge. Following this step, offenders familiarise themselves with the marketplace language and rules. To proceed with the crime, sellers then obtain or manufacture products to sell, then advertise the products. Once a transaction is completed, they receive the payment and then package and transport the products. Exchanging the currency or laundering the proceeds is sometimes necessary as well.

Sõmer, Hallaq and Watson (2016) developed a crime script using interviews conducted with cybercrime experts, law enforcement and academics. The crime script is a general version of a script on cybercrime equivalent to what is referred to as a protoscript in the literature (Cornish 1994). The authors constructed the script around three steps: preparation, execution and monetisation. The preparation step includes identifying potential victims, targeting social media and organising the attack. The execution step includes gaining access to systems and carrying out the attack. The monetisation step includes obtaining benefits such as direct monetary gain. Indirect monetary gain involves other offenders paying for services and goods obtained through the attack, victims paying the money and selling victim resources to other offenders.

Using court documents and expert interviews in the Netherlands, Matthijsse, van't Hoff-de Goede and Leukfeldt (2023) conducted a detailed crime script analysis of ransomware attacks deployed for financial gain. The first step involves creating a group to complete the ransomware attack, which generally consists of around 15 individuals, sometimes related to or known to each other. Many groups collaborate with different parties or 'outsource' parts of the process. The next step is setting up the infrastructure, which often involves hacking or hiring servers to host the botnet or ransomware infrastructure, setting up private communication channels so group members can communicate with each other, and obtaining stolen credit cards. This is followed by hiring malware developers to create the ransomware. Once developed, the ransomware can be used by the group, or sold or leased to other offenders. Attacks are usually untargeted. Offenders rather gain access to systems opportunistically. However, the focus is on companies or organisations because these are more lucrative.

A common method for gaining access is through a phishing or spam email inviting the victim to open an attachment or click on a hyperlink. This infects the computer and corrupts or encrypts backups. The offender conducts research on the target company to determine its revenue. The offender follows up by locating and exfiltrating data, including credentials and files that may be damaging to the victim. Encryption of the data follows, so inadequate backup procedures create vulnerability. After encryption, the extortion starts with offenders displaying a ransom note to and communicating with the victim. Offenders often pressure the victim to pay and threaten to leak data. The next step involves the victim paying the offenders, especially when critical files or backups were encrypted or to prevent the stolen data being leaked. When the victim has paid, offenders generally do not follow through on the threats and even assist the victim to decrypt the data. The final steps involve laundering the proceeds, often by using mixers (a mix of different types of cryptocurrencies) and/or exchanges and dividing the money among members of the group. Sometimes the money is reinvested in the ransomware campaign.

Discussion and conclusion

This review revealed important insights regarding crime scripts and offenders' methods of operation related to fraud facilitated by the internet—how offenders commit those crimes. Although relevant and insightful, many studies focused only on identifying a few stages or strategies that offenders used to commit crime rather than examining each step of the crime commission process. In this context, it is not possible to recreate the entire process from preparation to the execution of the crime, nor to identify the range of strategies offenders use throughout. Moreover, it was difficult to contextualise the use of these strategies and identify at which point in the process they were adopted, by whom and for what purpose. Some studies were particularly insightful because crime script analysis was used to reconstruct the crime commission process step by step in detail (see, for example, Loggen & Leukfeldt 2022; Matthijsse, van't Hoff-de Goede & Leukfeldt 2023).

What is known of the crime commission process of fraud facilitated by the internet?

The main goal of this study was to examine what is known of the crime commission process involved in different forms of fraud through script analysis and, by extension, identify important stages of the crime commission processes across different forms of fraud and whether those stages have been used to develop disruption or prevention measures. First, as illustrated in Table A1, fraud facilitated by the internet involves a complex sequence of steps, especially with the input of technology and use of various actors. Looking at the crime scripts identified in this literature, preparation and planning appear essential to understand. To carry out the crime, offenders must take steps such as setting up accounts and software, uploading a malicious application, recruiting telemarketers, developing a fraudulent scheme or creating a fake profile (Choi, Lee & Chun 2017; Hardy, Bell & Allan 2020; Hutchings & Holt 2015; Rege 2009; Van Hardeveld, Webber & O'Hara 2016). Depending on the crime, the commission step involves obtaining money from the victim using stolen information, sending images upon receiving payment, making a scam invoice by altering the bank account number on a real invoice or fabricating an entirely new invoice and persuading victims to transfer money (Choi & Lee 2021; Hutchings & Pastrana 2019; Junger, Wang & Schlömer 2020; Leukfeldt, Kleemans & Stol 2017; Soudijn & Zegers 2012; Whittaker & Button 2020).

Examining the crime scripts across the different forms of fraud highlights three important common elements. One stage observed across several types of fraud involves communication between the offender and the victim. Offenders will reach out to the victim by calling or sending an email or will approach a business (Choi & Lee 2021; Choi, Lee & Chun 2017; Junger, Wang & Schlömer 2020; Leukfeldt 2014; Van Nguyen 2022). This includes:

- making phone calls using automatic calling programs;
- speaking to victims by phone to carry out voice phishing (Choi, Lee & Chun 2017);
- contacting a financial employee while pretending to be a CEO and requesting that money be transferred into an account (Junger, Wang & Schlömer 2020);
- calling the victim while pretending to be a bank employee, for instance to obtain a transaction code in the case of phishing (Leukfeldt 2014; Loggen & Leukfeldt 2022; Van Nguyen 2022);
- communicating via email or a chat function on a ransom website or portal for ransomware (Matthijsse, van't Hoff-de Goede & Leukfeldt 2023); and
- simply reaching out to a victim online in the context of romance fraud (Rege 2009).

In some cases, the victim is deceived into contacting the offender, such as in online pet scams, in which victims contact a fraud offender they believe to be a legitimate pet store (Whittaker & Button 2020). Similarly, victims may inadvertently contact offenders when they reply to a phishing email or use a website that requires them to click on a link to obtain information (Choi & Lee 2021). In most cases, there is a point where the criminal group enters into direct contact with the victim for financial gain.

Another element common to most scripts involves using individuals outside of the immediate circle of offenders who act as 'enablers' and facilitate the commission of the crime (Leukfeldt, Kleemans & Stol 2017). This indicates that fraud and financial crime facilitated by the internet are highly dependent on other actors, partly due to the various technologies required. Potential enablers include money mules; recruiters; bank, postal and telecommunication employees; and callers contacting victims. Bank employees can provide offenders with information about potential victims while postal employees can intercept mail containing newly requested logins to online bank accounts (Leukfeldt, Kleemans & Stol 2017). Airline ticket fraud involves many other actors, such as a seller who operates in the online black market space, and a fake travel agent (Hutchings 2018). An online pet scam involves a fake pet shipping company (Whittaker & Button 2020).

Interestingly, the two most recent script analysis studies indicate that creating a criminal collaboration is a preliminary and essential phase of the fraud script (Loggen & Leukfeldt 2022; Matthijsse, van't Hoff-de Goede & Leukfeldt 2023), which is rarely discussed in the literature. In the case of ransomware, computer programmers and malware developers are recruited (Matthijsse, van't Hoff-de Goede & Leukfeldt 2023). More specifically, a core group of offenders develops the infrastructure and ransomware but will also buy access to a system from an initial access broker or even outsource the steps to other parties such as affiliates or negotiators. In phishing crimes, individuals with IT skills are often recruited as core members to build and maintain phishing websites. In addition, enablers can be recruited to obtain phishing software, to gather forged documents or the personal information of potential victims, or to call victims directly or intercept mail (Loggen & Leukfeldt 2022). Although it might be difficult to distinguish the main offenders leading the criminal activities from the enablers, committing these crimes appears unlikely without some of these enablers—an important point for prevention.

The third element common to several fraud types is the use of money mules, who act as a 'broker', moving money from victims to offenders (Leukfeldt, Kleemans & Stol 2017). The money is typically transferred from the victims to a money mule account, then transferred to an offender's account. Money mules break the money trail leading to core members of a criminal organisation. As observed with phishing attacks, money mules must be recruited to obtain their accounts (Loggen & Leukfeldt 2022). Groups of money mules can also be recruited from other countries for larger criminal operations. Once offenders have stolen bank card and financial data, they often transfer money to a money mule account (Soudijn & Zegers 2012; Van Nguyen 2022). The role of a mule can also extend to other fraudulent activities such as tax return fraud or multiple telephone subscriptions (Loggen & Leukfeldt 2022). Money mules can even directly collect the victim's payments in the case of some scams, such as an online pet scam (Whittaker & Button 2020). Without the bank accounts of money mules, the money would need to be transferred directly to offenders, which would put those offenders at high risk of being identified by the bank or the police.

Using crime scripts to prevent fraud facilitated by the internet

Communicating with the victim

With most forms of fraud, offenders (or criminal organisations) will communicate with the victim at some point. This includes making phone calls using an automatic calling program, calling the victim while pretending to be a bank employee to obtain transaction codes, or communicating via email or a chat function on a ransomware website. This appears to be a critical point in the script because offenders will often contact the victim directly—for instance, to obtain the money, in the case of ransomware. Matthijsse, van't Hoff-de Goede & Leukfeldt (2023) explain that encouraging or making it mandatory for victims to report victimisation and share information with authorities could increase the risks for offenders. Victims could also be given decryptors, allowing them to recover their data without paying the ransom.

Consistent with those suggestions, public awareness campaigns also appear important, educating potential victims on various forms of fraud and scams facilitated by the internet and what they could do to avoid being targeted and victimised. In a context where victims have acquired a minimum of knowledge on fraud and scams, a critical point might be for them to communicate with their financial institution (or other organisations, such as the Australian Taxation Office) as soon as an individual has contacted them to obtain personal information, to ensure that they are not targeted by offenders. Furthermore, if the public is aware that data recovery tools such as decryptors exist and are readily available, individuals will be less likely to be victimised. Finally, it could be made mandatory for customers of financial institutions to undertake brief online training on fraud and scams and how offenders may communicate with them to obtain their personal information. This would help to protect both the financial institution and potential victims by limiting the methods that offenders can use to communicate with victims.

Recruiting enablers

In empirical literature, the use of enablers to conduct fraud facilitated by the internet is relatively recent. Leukfeldt, Kleemans and Stol (2017) make a distinction between core members, professional enablers and recruited enablers. The core members (or main offenders) are initiating and coordinating the attacks on online banking. However, these offenders need professional enablers—that is, individuals providing services necessary to execute the criminal activities, such as developing malware. Recruited enablers are encouraged to provide services to the core offenders in exchange for a small fee. These services facilitate the crime commission by preventing the core offenders from exposing their identities while carrying out various parts of the script. Examples of recruited enablers include bank employees in call centres and postal workers.

Leukfeldt (2014) reported that banks could restrict employees' access to customers' personal data and either deliver mail themselves or use a reliable courier service. In addition, because recruited enablers contribute to the crime commission process, banks and post offices could offer annual educational programs to raise awareness among employees of how criminal organisations may try to recruit them. There is significant awareness of fraud and crime in the Australian financial sector—for example, suspicious matter reports increased 295 percent in 2016–17 (AUSTRAC 2022)—but financial institutions could be further educated on the detail of how cyber offenders conduct their criminal activities. At this stage, employees of banks or other financial institutions are commonly not trained specifically on recognising how offenders operate. Therefore, employees cannot identify criminal activities, make sense of the offender mindset or understand that criminal organisations could even try to recruit them. In this context, their capacity to monitor and prevent criminal activities is not maximised, which is why training is critical.

Using money mules

In 2021, Europol reported that incidents of money muling had grown 4.5 times since 2020, which demonstrates a dramatic increase in this problem globally. Money mules move money from victims' accounts to offenders' accounts so that offenders cannot be easily identified. As such, money mules are an important part of criminal activities. Money mules can be recruited in several ways, often through schools, social media and online job postings. Several studies have recommended awareness campaigns targeting potential money mules and focusing on the importance of not handing over an ATM card to anyone as well as the consequences of acting as a money mule (Hutchings & Pastrana 2019; Loggen & Leukfeldt 2022; Van Nguyen 2022). For instance, in 2009 the Australian Bankers' Association posted a warning for international students to help them avoid mule scams. One study also suggested that police and bank employees could pose as money mules (Soudijn & Zegers 2012), although the capacity of organisations to use this method is limited.

Awareness campaigns targeting potential money mules are a reasonable suggestion, especially to inform international students about this crime and its consequences. Another way to prevent the recruitment of money mules could be to reward students for intervening and preventing criminal activities. This is another way to use crime scripts for prevention purposes (see Leclerc 2014; Leclerc & Reynald 2017). For instance, offering monetary rewards or awards for civic engagement in the prevention of crime might encourage students not to act as money mules but rather as prevention agents. This latter suggestion might also boost commitment in financial institutions or other organisations where enablers could be recruited by criminal groups.

Suggestions for future research

Perhaps one critical point to discuss is the importance of recommending potential intervention measures to disrupt the script of offenders. Even though current literature on fraud facilitated by the internet revealed important insights into how offenders operate, very few studies examined measures that could be used to investigate, detect or prevent these crimes (Hardy, Bell & Allan 2020; Hutchings 2018; Van Nguyen 2022). This observation can also be made of the crime script literature on many crimes. Most script studies conducted to date focus on identifying the step-by-step sequence by which offenders operate without using this knowledge to suggest potential disruption or prevention measures (Leclerc 2016). This is despite the existence of previously published studies illustrating how to use each step to think about disruption or prevention of, for instance, drug manufacturing (Chiu, Leclerc & Townsley 2011), terrorism (Clarke & Newman 2006), child sexual abuse (Leclerc, Wortley & Smallbone 2011) and sexual offences against women (Chiu & Leclerc 2019, 2017). Furthermore, ideally, crime scripts for the same type of fraud, particularly complex fraud, should be reconstructed using different data samples to maximise the accuracy of the scripts and updated regularly based on emerging methods used by offenders. To our knowledge, script analysis research has not yet covered money laundering using cryptocurrency or stored value cards such as Amazon or Apple gift cards, which is now commonplace. This research would be valuable for gaining insights into these practices and how to disrupt them.

A final point is the relevance of data sharing to both understanding and disrupting criminal activities. An important initiative in this regard is the Australian Financial Crime Exchange, an independent, not-for-profit organisation formed by the four major banks to assist businesses to combat financial crimes. The exchange appears to be the primary channel through which the public and private sector can coordinate their intelligence and data-sharing activities for the investigation and prevention of financial crime and cybercrime. Consistent with this aim, having access to these data to reconstruct empirical-based crime scripts would be an important step. Without empirical data, the crime scripts (if constructed) cannot be used as efficiently to guide prevention initiatives. Talking to offenders is arguably the ideal data collection method for script analysis, simply because offenders are the main actors performing actions in the script (Leclerc 2016). Court documents, police reports, victim statements or even online forums can also be used to develop crime scripts. Matthijsse, van't Hoff-de Goede & Leukfeldt (2023) used a combination of court documents and interviews with cybersecurity experts. Leclerc et al. (2021) interviewed online police investigators. Another example is the study conducted by Aston et al. (2009), who used one year of data provided by one financial institution in Australia to produce a preliminary report on money mules. With the incredible rise in fraud, scams and other criminal activities facilitated by the internet, and the related exposure of financial institutions to criminal organisations, gathering and sharing data is an important step in better understanding how offenders operate and how to protect financial institutions and their customers from criminal activities and organised crime.

Conclusion

One way to boost capacity to investigate, prevent and detect fraud facilitated by the internet and financial crime is through crime scripting. Crime script analysis has now been applied to various categories of crimes including car theft (Morselli & Roy 2008), child sexual exploitation material on the darknet (Leclerc et al. 2021), domestic violence (Boxall et al. 2018) and illegal harvesting of live corals (Sosnowski, Weis & Petrossian 2020). Moreover, as observed in this review, researchers have started to apply crime scripts to fraud and financial crime globally, especially in the Netherlands by Leukfeldt and his colleagues. However, there is still a need for empirical research on how these crimes are committed and, most importantly, how each step of the script can identify measures that can lead to improved crime detection, reduction and prevention. Using online mandate fraud as an example, Donegan (2019: 770) reflects well on the potential of script analysis:

> Standardising investigation into digital fraud by mapping out digital criminality using crime scripts … could be beneficial for law enforcement. The results of this process could also assist in effectively identifying where law enforcement resources may be best deployed to solve some of the practical issues highlighted.

Arguably, this statement also applies to investigations conducted by financial institutions or other organisations.

To summarise, crime script analysis generates two key outcomes: a step-by-step account of the crime commission process that furthers our understanding of how offenders operate, and a framework for thinking of and applying detection, investigation and prevention strategies to disrupt these crimes. The strength of scripting relates to its simplicity and effectiveness in boosting the capacity of experts, financial investigators and institutions and law enforcement by providing a simple, practical framework that breaks down complex criminal processes, enriches our understanding of offenders' strategies and leads to improved strategies for crime detection, reduction and prevention. Crime script analysis offers a complementary framework to understand and disrupt crime.

References

URLs correct as at September 2023

Aston M, McCombie S, Reardon B & Watters P 2009. A preliminary profiling of internet money mules: An Australian perspective. In *2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, Brisbane: 482–487. https://doi.org/10.1109/UIC-ATC.2009.63

AUSTRAC 2022. *AUSTRAC 2020–21 annual report*. https://www.austrac.gov.au/about-us/corporate-information-and-governance/annual-reports

Australian Bureau of Statistics 2016. *Personal fraud, 2014–15*. ABS cat. no. 4528.0. Canberra: Australian Bureau of Statistics. https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud

Australian Competition and Consumer Commission 2023. *ACCC welcomes funding to establish National Anti-Scam Centre*. Media release, 15 May. https://www.accc.gov.au/media-release/accc-welcomes-funding-to-establish-national-anti-scam-centre

Australian Securities and Investments Commission 2020. *ASIC obtains interim injunctions against Larry Dawson and PW Kitt Co Pty Ltd*. Media release, 19 August. https://asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-187mr-asic-obtains-interim-injunctions-against-larry-dawson-and-pw-kitt-co-pty-ltd/

Boxall H, Boyd C, Dowling C & Morgan A 2018. Understanding domestic violence incidents using crime script analysis. *Trends & issues in crime and criminal justice* no. 558. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi558

Broadhurst R & Trivedi H 2020. Malware in spam email: Risks and trends in the Australian Spam Intelligence Database. *Trends & issues in crime and criminal justice* no. 603. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04657

Burgard A & Schlembach C 2013. Frames of fraud: A qualitative analysis of the structure and process of victimization on the internet. *International Journal of Cyber Criminology* 7(2): 112–24

Cale J, Holt T, Leclerc B, Singh S & Drew J 2021. Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends & issues in crime and criminal justice* no. 617. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04893

Chiu Y-N & Leclerc B 2019. Scripting stranger sexual offenses against women. *Sexual Abuse: A Journal of Research and Treatment* 33(2): 223–49. https://doi.org/10.1177/1079063219889055

Chiu Y-N & Leclerc B 2017. An examination of sexual offenses against women by acquaintances: The utility of a script framework for prevention purposes. In B Leclerc & E Savona (eds), *Crime prevention in the 21st century.* Cham: Springer: 59–76. https://doi.org/10.1007/978-3-319-27793-6_6

Chiu Y-N, Leclerc B & Townsley M 2011. Crime script analysis of drug manufacturing in clandestine laboratories: Implications for strategic intervention. *British Journal of Criminology* 51(2): 355–374. https://doi.org/10.1093/bjc/azr005

Choi K, Lee JL & Chun YT 2017. Voice phishing fraud and its modus operandi. *Security Journal* 30(2): 454–466. https://doi.org/10.1057/sj.2014.49

Choi Y-J & Lee J 2021. The change in the methods of smishing in South Korea after the onset of covid-19. *Journal of Legal, Ethical and Regulatory Issues* 24: 1–12

Clarke RV 2008. Situational crime prevention. In R Wortley & L Mazerolle (eds), *Environmental criminology and crime analysis*, 1st edition. Cullompton, UK: Willan: 178–194

Clarke RV & Newman G 2006. *Outsmarting the terrorist.* Westport, CT: Praeger Security International

Cornish DB 1994. The procedural analysis of offending and its relevance for situational prevention. In RV Clarke (ed), *Crime prevention studies* vol. 3. Monsey, NY: Criminal Justice Press

Cornish DB & Clarke RV 2002. Analyzing organized crimes. In AR Piquero and SG Tibbetts (eds), *Rational choice and criminal behavior: Recent research and future challenges*. New York, NY: Routledge: 41–63

Donegan M 2019. Crime script for mandate fraud. *Journal of Money Laundering Control* 22(4): 770–781. https://doi.org/10.1108/JMLC-03-2019-0025

Drew JM & Drew ME 2010. The identification of Ponzi schemes: Can a picture tell a thousand frauds? *Griffith Law Review* 19: 51–70. https://doi.org/10.1080/10854668.2010.10854668

Ekblom P & Tilley N 2000. Criminology, situational crime prevention and the resourceful offender. *British Journal of Criminology* 40: 376–398. https://doi.org/10.1093/bjc/40.3.376

Emami C, Smith RG & Jorna P 2019. *Online fraud victimisation in Australia: Risks and protective factors*. Research Report no. 16. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/rr09319

Europol 2021. European money mule action leads to 1803 arrests. https://www.europol.europa.eu/media-press/newsroom/news/european-money-mule-action-leads-to-1-803-arrests

Grand View Research 2023. Cyber security market size, share & trends analysis report by component, by security type, by solution, by services, by deployment, by organization size, by applications, by region, and segment forecasts, 2023 – 2030. https://www.grandviewresearch.com/industry-analysis/cyber-security-market

Hardy J, Bell P & Allan D 2020. A crime script analysis of the Madoff Investment Scheme. *Crime Prevention and Community Safety* 22(1): 68–97. https://doi.org/10.1057/s41300-019-00082-6

Hutchings A 2018. Leaving on a jet plane: The trade in fraudulently obtained airline tickets. *Crime, Law and Social Change* 70(4): 461–487. https://doi.org/10.1007/s10611-018-9777-8

Hutchings A & Holt TJ 2015. A crime script analysis of the online stolen data market. *British Journal of Criminology* 55(3): 596–614. https://doi.org/10.1093/bjc/azu106

Hutchings A & Pastrana S 2019. Understanding eWhoring. In *2019 IEEE European Symposium on Security and Privacy*, Stockholm, Sweden: 201–214. https://doi.org/10.1109/EuroSP.2019.00024

Internet Society's Online Trust Alliance 2019. *2018 Cyber incident & breach trends report*. https://www.internetsociety.org/breach2019/

Junger M, Wang V & Schlömer M 2020. Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science* 9(1): 1–15. https://doi.org/10.1186/s40163-020-00119-4

Leclerc B 2017. Boosting crime scene investigations capabilities through crime script analysis. In Q Rossy, D Décary-Hétu, O Delémont & M Mulone (eds), *Routledge international handbook of forensic intelligence and criminology*. London: Routledge. https://doi.org/10.4324/9781315541945

Leclerc B 2016. Crime scripts. In R Wortley and M Townsley (eds), *Environmental criminology and crime analysis*, 2nd edition. London: Routledge: 119–141. https://doi.org/10.4324/9781315709826

Leclerc B 2014. Script analysis for crime controllers: Extending the reach of situational crime prevention. In S Caneppele & F Calderoni (eds), *Organized crime, corruption and crime prevention*. New York: Springer. https://doi.org/10.1007/978-3-319-01839-3_2

Leclerc B, Drew J, Holt T, Cale J & Singh S 2021. Child sexual abuse material on the darknet: A script analysis of how offenders operate. *Trends & issues in crime and criminal justice* no. 627. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78160

Leclerc B & Reynald D 2017. When scripts and guardianship unite: A script model to facilitate intervention of capable guardians. *Security Journal* 30: 793–806. https://doi.org/10.1057/sj.2015.8

Leclerc B & Wortley R (eds) 2013. *Cognition and crime: Offender decision making and script analyses*. Crime Science Series. London: Routledge. https://doi.org/10.4324/9780203083482

Leclerc B, Wortley R & Smallbone S 2011. Getting into the script of adult child sexual offenders and mapping out situational prevention measures. *Journal of Research in Crime and Delinquency* 48(2): 209–237. https://doi.org/10.1177/0022427810391540

Lee JR & Holt T 2020. The challenges and concerns of using big data to understand cybercrime. In B Leclerc & J Cale (eds), *Big data*. London: Routledge: 85–103. https://doi.org/10.4324/9781351029704

Leukfeldt ER 2014. Cybercrime and social ties. *Trends in Organized Crime* 17(4): 231–249. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt ER, Kleemans ER & Stol WP 2017. A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change* 67(1): 21–37. https://doi.org/10.1007/s10611-016-9662-2

Levi M 2008. Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology and Criminal Justice* 8(4): 389–419. https://doi.org/10.1177/1748895808096470

Levi M & Smith RG 2021. *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*. Research Report no. 19. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/rr78115

Loggen J & Leukfeldt R 2022. Unraveling the crime scripts of phishing networks: An analysis of 45 court cases in the Netherlands. *Trends in Organized Crime* 25: 205–225. https://doi.org/10.1007/s12117-022-09448-z

Matthijsse SR, van't Hoff-de Goede MS & Leukfeldt ER 2023. Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*. Advance online publication. https://doi.org/10.1007/s12117-023-09496-z

Moher D, Liberati A, Tetzlaff J, Altman DG & PRISMA Group 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Med* 6(7): e1000097. https://doi.org/10.1371/journal.pmed.1000097

Morselli C & Roy J 2008. Brokerage qualifications in ringing operations. *Criminology* 46: 71–98. https://doi.org/10.1111/j.1745-9125.2008.00103.x

National Audit Office 2017. *Online fraud*. HC 45. London: National Audit Office. https://www.nao.org.uk/report/online-fraud/

Rege A 2009. What's love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology* 3(2): 494–512

Sõmer T, Hallaq B & Watson T 2016. Utilising journey mapping and crime scripting to combat cybercrime and cyber warfare attacks. *Journal of Information Warfare* 15(4): 39–49

Sosnowski M, Weis JS & Petrossian GA 2020. Using crime script analysis to understand the illegal harvesting of live corals: Case studies from Indonesia and Fiji. *Journal of Contemporary Criminal Justice* 36(3): 384–402*.* https://doi.org/10.1177/1043986220910295

Soudijn MR & Zegers BCT 2012. Cybercrime and virtual offender convergence settings. *Trends in Organized Crime* 15(2): 111–129. https://doi.org/10.1007/s12117-012-9159-z

Van Hardeveld GJ, Webber C & O'Hara K 2016. *Discovering credit card fraud methods in online tutorials.* Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention. Hannover, Germany: Association for Computing Machinery: 1–5. https://doi.org/10.1145/2915368.2915369

Van Nguyen T 2022. The modus operandi of transnational computer fraud: A crime script analysis in Vietnam. *Trends in Organized Crime* 25: 226–247. https://doi.org/10.1007/s12117-021-09422-1

Whittaker JM & Button M 2020. Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. *Australian & New Zealand Journal of Criminology* 53(4): 497–514. https://doi.org/10.1177/0004865820957077

Appendix

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet

Study and country	Data source	Findings	Crime intervention
Burgard & Schlembach (2013) Austria	30 victim interviews	Perspective of the victim • Victims' risk perception decreased and motivation to receive rewards offered increased • Fraudster decreases feelings of distrust in victim	
Choi & Lee (2021) South Korea	280 recounts by victims posted on websites popular in South Korea (Naver, Daum, Google, YouTube)	Crime script of smishing • pre-crime phase – purchasing victim personal information – preparation of attack through arranging, setting up and uploading malicious apps • sending message – send message with link to website where malicious app is uploaded – download of malicious app on victim's smartphone and theft of personal info – attempt financial gain by using victim's stolen info – charge payments to victims Offenders used new methods of smishing after the onset of the COVID-19 pandemic, such as delivery of free masks or reservation of vaccines.	
Choi, Lee & Chun (2017) South Korea	• 182 police cases • 229 victim accounts uploaded on forums • 20 interviews with detectives involved in voice phishing investigations	Crime script for voice phishing • pre-crime: preparation of criminal organisations, recruitment of telemarketers • crime event: making phone calls (usually through an automatic calling program), conversations (varied approaches) • post-offence: deposit and withdrawal, money transfer	Warning messages for unidentified or suspicious internal internet calls

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Hardy, Bell & Allan (2020) USA	• 97 articles • 72 sworn affidavits • 61 interview transcripts • 10 New York district court transcripts	Madoff investment scheme crime script • development of a functioning scheme (devise investment scheme, establish business structures, create trading accounts, market entry) • misappropriation of funds (victim screening, communication and recruitment, receiving victim funds) • continuation of the Ponzi element of fraud (victim payments, fabricating investment reports, false trading records, collapse)	Challenge biases about likely offenders Promote awareness of fraudulent schemes Increase access to due diligence information and services Assist victim communities to report suspicious offers
Hutchings (2018) Multi-country	• 13 interviews with stakeholders • Excerpts of black market advertisements, buyer feedback and commentary	Crime scripts involved in trade of fraudulently obtained airline tickets • act 1: preparation – actors: victim traveller, complicit traveller, mule handler, re-seller – variants online black markets, fake travel agency, insider word-of-mouth • act 2: the middle-men and methods – actors: black market seller, fake travel agent, rogue employee – variants: compromised credit cards, loyalty point fraud, unauthorised access to global distribution systems, compromised business accounts, identity fraud, voucher fraud • act 3: travelling or attempting to travel – actors: victim traveller, complicit traveller, mule – tracks: cancelled booking, detained by law enforcement, providing information, travelling successfully, involvement in other crime	Potential alternative intervention Increase difficulty of changing account details such as by using multifactor authentication Airline blacklists of those repeatedly travelling or attempting to travel on fraudulently purchased tickets Taking down websites of fake travel agencies

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Hutchings & Holt (2015) N/A	Snowball sampling of 13 stolen data forums	Crime script for selling stolen data (sellers, buyers, moderators) • preparation: setting up necessary software and creating accounts, ensuring anonymity and security, locating marketplace, learning specialist knowledge • entry: learning marketplace language and rules • pre-condition: obtaining and manufacturing products to sell • instrumental pre-condition: advertising and verifying products and services • instrumental initiation: exchanging law enforcement information, negotiation and communication • instrumental actualisation: sending and receiving payment • doing: packaging and transporting goods • post condition: reputation management, exchanging currency • exit: laundering proceeds	
Hutchings & Pastrana (2019) N/A	6,519 forum posts of guides and tutorials from underground forums	Crime script for 'eWhoring' • preparation: learn techniques • entry: obtain images • pre-condition: create an alias and prepare a backstory, open accounts, customise images (optional) • instrumental pre-condition: source traffic • instrumental initiation: negotiate • instrumental actualisation: receive money • doing: send images • post condition: block or continue to milk customers • exit: exchange funds Alternative tracks: blackmail, affiliate marketing, sending malware, scams	Promote distrust relating to tutorials Increase likelihood of image saturation Verify accounts and shut down for misuse

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Junger, Wang & Schlömer (2020) Netherlands	100 randomly sampled cases for three types of fraud from Dutch non-profit organisation	Crime scripts • CEO fraud – select and conduct research on company – spoof email address of CEO – contact financial employee posing as CEO and request money transfer to account – push employee to transfer • fraudulent contract – select and conduct research on company – approach and persuade business to accept advertisement opportunity – ensure verbal or signed agreement – start sending invoices to business per payment terms – push business to pay invoices as per agreement • ghost invoice – select and conduct research on company – fabricate an invoice or alter the bank account details of a real invoice – send invoice to company – wait and check whether the business pays invoice	Current preventative measures discussed, none suggested based on crime script
Lee (2021) China	Posts on Chinese forum platform Baidu Tieba	Crime script of customer-to-customer fraud • pre-operation: familiarisation and trust management between vendors and customers • operation: discussing deals • finalisation and exit: victim sends money and vendor disappears	
Leukfeldt (2014) Netherlands	• Case study of a criminal group • Records of interrogations obtained during investigation • Interviews with criminal justice actors	Crime script of phishing • send emails to potential victims appearing to be from the victim's bank asking them to click on a link to a phishing website • to obtain transaction code, using information provided by victim, offender calls victim posing as a bank employee to obtain a transaction. Victim shares the code, enabling access to account • upon receiving the code, the offender transfers the money from the victim's account to their account	Awareness campaigns to prevent money mules from participating Increased security levels for call centre staff

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Leukfeldt, Kleemans & Stol (2017) Netherlands	Police files of 18 cases of criminal investigations	Commonalities among scripts of crime networks engaged in attacks on online banking • intercept login credentials from victims to gain access to online bank accounts • obtain one-time authentication codes • transfer money from the victim's account to accounts of money mules • money cashed out • use of phishing emails and websites which require the victim to reply by email or click on a link to obtain information. Offender poses as bank employee and asks for authentication codes to subsequently transfer money from victim's bank accounts to money mule accounts. Low-tech attacks with a low degree of victim–attacker interaction • victim receives a phishing email with a link to a phishing website and enters information. The telephone number entered by the victim is used to obtain a new SIM card. Authentication codes are sent to the mobile phone of the offenders and money is transferred from the victim's bank account. High-tech attacks with a high degree of victim–attacker interaction • offenders infect a victim's computer and gain control over it using malware that does not require interaction. The malware is spread via emails containing links. High-tech attacks with a low degree of victim–attacker interaction • the offender exploits a website with outdated security. When the potential victim accesses the website, their computer is infected, allowing access to their bank account.	Suggestions from other studies included

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Loggen & Leukfeldt (2022) Netherlands	45 court cases	Crime script for phishing attacks • forming a criminal group • obtaining resources and specific services necessary for the phishing attack • preparing for the theft of ATM cards • recruiting money mules and obtaining money mule accounts • making contact with potential victims and distributing attack materials • theft of personal information • obtaining ATM cards from victims • obtaining verification codes to transfer money and to install the mobile banking app • withdrawing money using victims' ATM cards • transferring money to money mule accounts or accounts of companies • reselling goods purchased with illegally-obtained money • spending the illegally-obtained funds	Increase the difficulty of obtaining resources aiding in the phishing attack and the risk of criminals being caught by bank employees Paying attention to chat services, such as Telegram Banks to deliver the mail themselves or use a highly reliable courier service Warning banners displayed by search engines when people search for instructions on creating phishing software Closing forums where such services and tools are advertised Awareness campaign on money muling Social media companies to monitor activities on websites used to recruit money mules

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Matthijsse, van't Hoff-de Goede & Leukfeldt (2023) Netherlands	44 court documents and interviews with 10 international experts (public organisations and cybersecurity companies)	Crime script for ransomware attacks • form criminal collaboration • set up infrastructure • develop ransomware • sell ransomware • select target • gain access • infect victim's computer • data exfiltration • encryption • extortion • communication • cash-in • launder money • pay collaborators and reinvest	Security measures such as timely vulnerability patches, antivirus and monitoring, but also awareness and training of employees Disrupting the ransomware-as-a-service market or regulating cryptocurrency mixers and exchanges Legislation making it mandatory for victims to report victimisation and share information with the authorities Providing victims with decryptors to recover their data without paying the ransom Securing or isolating sensitive data to prevent data extortion or disrupting the initial access market Back-ups and data recovering strategy
Rege (2009) N/A	170 internet documents	Crime script for romance scams • design a fake profile • initiate communication and establish a strong bond with victims • request money using narratives of tragic or desperate circumstances • continue until victims lose patience or realise they have been scammed and stop sending money Many individuals were involved in groups of scammers who pooled money, shared internet access and resources and trained others.	

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Sõmer, Hallaq & Watson (2016) Various European countries	Interviews with experts on cybercrime and law enforcement	General cybercrime script • preparation phase – deciding to engage in criminal activity – choosing a victim – choosing a method • execution phase: conducting the crime • monetisation/reward phase: exiting	
Soudijn & Zegers (2012) Netherlands	Carding forum posts	Crime script of carding where offenders obtain money with stolen financial information • preparation: partnerships developed and infrastructure set up • theft: case used phishing method • money transferred to bank accounts of money mules in small amounts • cashing: carder employs others to withdraw and deposit cash into a deposit box which is collected by the carder	Closing carding forums Infiltrating forums Creating lemon market (an online market where buyers cannot be certain of product quality) Raising awareness among potential victims
Van Hardeveld, Webber & O’Hara (2016) N/A	25 tutorials on darknet forums	Crime script for purchasing and using stolen credit card details (selected steps) • find forums, set up pseudonymous account, read through posts and obtain cryptocurrency to pay for tutorials if necessary • ensure security with the use of VPNs, SOCKS5, virtual machines • buy stolen credit card details on carding forums on both clear web and darknet • find ‘cardable’ websites, belonging to either large online retailers or small businesses • cash out cards: obtain physical goods, money, services or vouchers • protect security and reputation by leaving a review on the forum	Seize illicit forums Motivate online retailers to increase security Discuss effects of carding on victims with offenders

Table A1: Studies using crime script analysis to investigate fraud facilitated by the internet (cont.)

Study and country	Data source	Findings	Crime intervention
Van Nguyen (2022) Vietnam	• Snowball sampling • Semi-structured interviews with police officers	Crime script for bank card data fraud • preparation: source bank card data, recruit money mules and other members, prepare tools • activity: online purchases, counterfeit cards • post-activity: flee • Crime script for phone scams • preparation: recruit members, prepare tools and locations • activity: make fraudulent calls to victims, receive money illegally • post-activity: flee	Transnational cooperation Raise citizens' awareness Awareness-raising for potential supporting offenders
Whittaker & Button (2020) Australia, United States, South Africa	415 pet deposit complaints made to petscams.com	Crime script of pet scams • use of legitimate appearance of fraudulent pet website • first contact made by victim • communication occurred through email, phone calls, text or WhatsApp • use of pre-scripted fictional business history, after-sale documentation and pet wellbeing items • following trust building, victims pressured into making deposit for reasons such as same-day delivery • low price of pets which offender alleviated through excuses (being the first litter) • money requested to be sent to non-refundable platforms which often had to be collected in the US by mules • $300–$1,500 transferred in deposit stage • Secondary recurring fees: 'the sting' • recontacted by fake shipping company and for other fictitious costs • threatening the buyer with fines and recurring fees such as special shipping fees for flying during COVID-19 lockdown	

Dr Benoit Leclerc is Professor of Criminology and Criminal Justice at Griffith University.

Elena Morgenthaler is a PhD Candidate at the School of Criminology and Criminal Justice at Griffith University.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website: www.aic.gov.au

ISSN 1836-2206 (Online)   ISBN 978 1 922877 20 8 (Online)

https://doi.org/10.52922/ti77208

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government

www.aic.gov.au