Summaries

Justitiële verkenningen (Judicial explorations) is published six times a year by the Research and Documentation Centre of the Dutch Ministry of Justice and Security in cooperation with Boom juridisch. Each issue focuses on a central theme related to judicial policy. The section Summaries contains abstracts of the internationally most relevant articles of each issue. The central theme of this issue (no. 2, 2020) is *New forms of swindling and fraud.*

Corona crisis and fraud: four possible relationships
Clarissa Meerts and Wim Huisman
This contribution contains several concrete examples of 'Corona crime' thereby showing how the current crisis is creating new opportunities for committing crimes. The authors revert to an analysis framework that was previously used to interpret new forms of crime during the banking crisis. It consists of four scenarios that are briefly described. The future will have to show what effects the corona pandemic has had on fraud and other financial and economic crime.

Fishing with a new rod: an investigation into payment request fraud
Joke Rooyakkers and Marleen Weulen Kranenbarg
Online fraudsters seem to adapt to new digital opportunities. While the academic literature about phishing mainly focuses on phishing through emails, fraudsters also appear to use new means of communication and platforms to find and deceive their victims. Based on analysis of 728 police reports from the period from June 20th to August 20th 2019, this article provides a descriptive study on the new phenomenon of payment request fraud on the Dutch advertisement platform Marktplaats.nl (similar to eBay). The article will provide a thorough description of the crime script and its success factors. As fraudsters now use new means of communication, it will also be assessed to what extent they use new persuasion techniques, and to what extent victims may have different characteristics. The research, therefore, focuses on the modus operandi, persuasion techniques used by the fraudsters, and victim characteristics.

Fraud and scams on Telegram Messenger. Results from a netnographic study

Robby Roks and Nahom Monshouwer

In this article, the authors draw on a *netnographic* study conducted between May and July 2019 on phishing on Telegram Messenger. The results indicate that Telegram, just like cryptomarkets and online forums, seems to function as a criminal marketplace. In the groups analyzed the authors see users who both offer and are looking for specific goods and services related to the crime script of phishing. Furthermore, the information on Telegram contains specific modi operandi that are offering comprehensive and step-by-step guides to successfully complete specific financial cybercrimes. Therefore, based on this explorative study the authors argue that Telegram can be seen as a digital offender convergence setting.

Romance scams, dating fraud and 'sweetheart swindles'. The loss of money, happiness and face

Raoul Notté

Romance scams have seen a worldwide increase and are one of the most financially damaging forms of cybercrime. In addition, victims suffer strong emotional impact and are confronted with victim blaming. Research shows how the combination of various emotional and financial impact can induce a 'double-hit' on victims. Knowledge and possibilities for law enforcement are insufficient, which leads to a lack of financial compensation and support for victims.

Who will get their money back? Victims' actions for compensation in bank fraud

Johan van Wilsem, Take Sipma and Esther Meijer-van Leijsen

In the Internet era, banking fraud has become a common way of stealing money. According to victim surveys, this offense has already led to significant numbers of victims. In this article, the authors focus on illegal bank account withdrawals, which are an indication of identity fraud. For this they use data on 636 victims who were surveyed in the LISS panel. Using the concept of 'capability to act', as used in the WRR report *Why knowing what to do is not enough* (2017), the authors model which type of victim takes action to get the stolen amount reimbursed and which type of victim succeeds in doing so. They expect that the less educated and people with low self-control more

often refrain from contact with authorities (bank, police) and therefore more often receive no compensation and remain with higher residual damage. The results show that approximately four in five victims of unauthorized bank debits are fully compensated. For the group of victims for whom this is not the case – remaining with residual damage – most of the hypotheses are confirmed.

Social engineering: digital fraud and deception

Jan-Willem Bullée and Marianne Junger

The prevalence of online crime increases. Social engineering, such as email phishing, is often an important element in an attack. Several interventions have been developed to reduce the success of these types of attacks. The current study investigates whether interventions can help reduce vulnerability to social engineering attacks. The authors investigate which types of interventions and specific elements are most successful. They selected studies with an experimental design that tested at least one intervention. A total of 19 studies with 37 effect sizes, based on a total sample of N=23,146 subjects, were found. The available training courses, intervention materials and effect sizes were analysed. Overall, positive effects of interventions were found. However, there are substantial differences in effect for the different types of interventions. Effective interventions are relatively intensive and have a specific focus. The authors conclude with the design of the best possible intervention given the results of their research.

Our cyber behavior is much more unsafe than we think. Implications for effective government influence policy

Rick van der Kleij, Susanne van 't Hoff-de Goede, Steve van de Weijer and Rutger Leukfeldt

The aim of this research was to examine how Dutch citizens behave online and to explain their online behavior. The results of an experimental survey (N=2,426) show that unsafe behavior is highly prevalent. For example, nearly 40% of the respondents use a weak password. However, it appears that there are major differences between self-reported behavior and objective behavior. The objective measurements in the survey show that people behave more unsafely than they self-report. The research further shows that there is no silver bullet for promoting more safe online behavior. Different online behaviors seem

to stem from different sources. Nevertheless, the authors do see a lot of value in interventions that focus on adaptations to the technology that people use for online activities, such that the possibility of unsafe behavior is reduced and the possibility of safe behavior is increased – also known as *security by design*. There is a role here for policy measures encouraging technology manufacturers to make these adjustments.