Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram

Luuk M. J. Bekkers (https://orcid.org/0000-0002-3447-5245) [1]

Asier Moneva (https://orcid.org/0000-0002-2156-0213) [1, 2]

E. Rutger Leukfeldt (https://orcid.org/0000-0002-3051-0859) [1, 2]

[1] *Center of Expertise Cyber Security, The Hague University of Applied Sciences*

[2] *Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)*

Correspondence: Center of Expertise Cyber Security, The Hague University of Applied Sciences. Johanna Westerdijkplein 75, 2521 EN Den Haag. Email: l.m.j.bekkers@hhs.nl

Abstract

Objectives: Examine the level of engagement of young users with money mule recruitment ads on Instagram.

Methods: Three ads reflecting key cybercrime involvement mechanisms and targeting Dutch user clusters were run on two Instagram placements. By means of this quasi-experimental 3 x 2 factorial design, we were able to analyze the reach and views of the ads, click-through rates, gender of the participants and temporal distributions of user engagement.

Results: Mimicking actual recruitment environments, analysis shows that up to three percent of young users engaged with the ads, especially those promoting a luxury lifestyle and using neutralization techniques. Men were more likely to engage, and click-through rates were higher at night.

Conclusions: Some young Instagram users seem prone to making money through their bank cards and risk becoming involved in cybercrime online. We encourage future research to explore further the use of social media in criminological studies.

Keywords: Ad engagement, Instagram, cybercrime, involvement mechanisms, money mules, online recruitment, situational crime prevention

1. Introduction

Social networking is one of the most popular activities on the Internet. In the Netherlands, almost every citizen between 12 and 45 years of age is thought to use social media (Statistics Netherlands 2021). Also in other countries, from emerging and developing economies to those more advanced, social media usage continues to rise (Poushter et al. 2018). Social media allows people to connect more easily with friends, family, and strangers, both nationally and internationally. Unfortunately, such possibilities are also exploited by criminals. Digitization leads to new criminal opportunities and reinforces the modus

operandi of criminals operating in the offline world (Maimon and Louderback 2019; Moule et al. 2013; Roks et al. 2021). For instance, criminal networks use social media to communicate with co-offenders and to recruit new members. As a result, social media has a major impact on how these networks are structured and who becomes a part of them (de Boer et al. 2022; Roks et al. 2021).

Specifically, social media play a key role in the formation of criminal networks through the recruitment of money mules (Bekkers and Leukfeldt 2022; Roks et al. 2021). Money mules can be defined as individuals who provide criminals with access to their bank account (Aston et al. 2009; Dunham 2006; Europol 2021). Bank accounts are then used to obscure the financial trail between offenders and victims. Money acquired via phishing, online fraud, or other types of financially-motivated cybercrimes is directly transferred from the bank account of the victim to the bank account of the money mules, after which the funds are often withdrawn as quickly as possible (Bulanova-Hristova et al. 2016; Custers et al. 2019; Leukfeldt 2014; Leukfeldt et al. 2017a, 2017b, 2017c; Leukfeldt and Holt 2022). In this way, criminals remain anonymous and avoid detection by banks and law enforcement, while money mules take all the risk.

There are many examples on social media accounts of criminals using a variety of advertising techniques to convince users to provide their bank account details to criminal networks, in which young adults form a particularly vulnerable target group (Bekkers and Leukfeldt 2022; Roks et al. 2021). Engaging with these types of advertisements can thus lead to the involvement into cybercrime. Bekkers and Leukfeldt (2022) provided a qualitative examination of the online involvement mechanisms of cybercrime by analyzing how money mule recruiters advertise on Instagram. It appears that most recruiters do not deem it necessary to pro-actively reach out to the target group; once an online network has been established, money mules find their way to the recruiters. The authors found that most of the money mule recruitment accounts on Instagram revolve around a luxurious lifestyle subculture. Those accounts use, for instance, images of money bundles and expensive accessories and claim lots of money is to be earned. In other

cases, recruiters active online seek to normalize money muling by stating that others have engaged in it before, all the while portraying themselves as regular businesspeople. Sometimes recruiters use techniques that neutralize the illegality of money muling, implying that the online target group is aware of the risks and yet participates willingly. It is by using the aforementioned techniques that recruiters try to convince Instagram users to contact them and provide their bank account details.

Due to a lack of research, however, it is currently unknown to what extent users are tempted to give their account details to recruiters online. This information could be used to prevent people from becoming involved in cybercrime as money mules, thereby intervening with the crime script of many different financially motivated cybercrimes. To better understand how money mules are recruited on social media and identify the key online involvement mechanisms, this paper presents the results of a unique quasi-experiment that examines the engagement of young Dutch Instagram users with three online advertisements (hereafter referred to as 'ads') that replicate the ones actual criminal networks use to recruit money mules on this social media platform. The rest of the paper begins with a theoretical overview of current insights into the online and offline involvement mechanisms of (cyber)crime and the phenomena of money muling. Thereafter, we describe the design and results of two quasi-experiments, followed by an interpretation of the findings and a discussion on their theoretical and practical implications.

2. Cybercrime Involvement Mechanisms and Money Mules

The involvement mechanisms of crime, together with individual sequences of offending and (dis)continuity in criminal trajectories, is one of main lines of research on organized crime careers in developmental and life-course criminology (Kleemans and de Poot 2008; Kleemans and van Koppen 2020). It has long been argued that new members often become involved in organized crime via existing social ties (Calderoni et al. 2020; Campedelli et al. 2021; Ianni and Reuss-Ianni 1972; Kleemans and de Poot 2008; Kleemans and van Koppen 2020; Morselli 2005; Paoli 2003). For instance, in the cases of

Dutch organized crime and the Italian mafia, newly recruited individuals join the same criminal network where kinship relations or other close social ties are present (Campedelli et al. 2021; Kleemans and de Poot 2008; van Dijk et al. 2019; van Koppen 2013). Social ties provide opportunity to engage in crime and help to establish a basic level of trust, something that is inherently lacking in risky criminal environments (Kleemans and de Poot 2008; Kleemans and van Koppen 2020). Indeed, social relations allow access to co-offenders and individuals whose jobs or knowledge are used to execute parts of sometimes complex crime scripts. It is therefore not surprising that intervening in socialization processes by severing criminal ties leads to significant reductions in new recruits (Calderoni et al. 2022). Additionally, "offender convergence settings," such as bars and cafes, are used to get in touch with individuals outside one's initial social cluster, considering the limited capabilities and other restrictions associated with existing relationships (Felson 2003). These settings allow criminals to establish links, to find new members and to forge new alliances.

The ongoing digitization of crime has also affected the processes of involvement into crime. Research shows that, while the origin and growth of cybercriminal networks is still often anchored in social ties in the physical world, criminals shift their activities increasingly to the online world to find suitable co-offenders (Hutchings and Holt 2015; Leukfeldt et al. 2017a, 2017b, 2017c; Leukfeldt and Holt 2022; Roks et al. 2021). Social media platforms provide opportunities to reach potential new members, which is evident in the case of money mules. The extant literature identifies three main online involvement mechanisms: normalization of the behavior, looking up to a luxury lifestyle, and neutralization techniques (Bekkers and Leukfeldt 2022; Leukfeldt and Kleemans 2019; Roks et al. 2021). While these were initially identified as offline cybercrime involvement mechanisms, preliminary evidence shows that online recruiters also exploit them—although it is unknown if and why youth engage with these recruiters (Bekkers and Leukfeldt 2022).

Money mules are often part of a subculture in which participating in acts of fraud is tolerated (Bekkers and Leukfeldt 2022; Leukfeldt and Kleemans 2019; Roks et al. 2021). Groups with specific norms, values, and traditions that oppose the dominant culture, are subcultures, which evolve as a rejection to the dominant culture or around certain phenomena that the larger society might not support (Brake 2013; Holt 2007; Quinn and Forsyth 2005). Statements from money mules show they find it normal to be approached by members of a criminal network in their local neighborhood, sometimes even daily (Leukfeldt and Kleemans 2019). Money mules do not always give in right away, but some eventually do so. Hence, illegal behavior seems to be morally acceptable; it is normalized in such social environments, which increases the likelihood of bystanders exhibiting the same behavior (Herbert 1998; Pratt et al. 2010). Recruiters on Instagram normalize money muling by pointing users to past success, for instance by showing previous bank transfers, or by framing themselves as a safe and reliable company in search of cooperation (Bekkers and Leukfeldt 2022).

Part of the subculture is that mules look up to the luxurious lifestyle of criminals. Money mules desire the expensive clothes and cars that criminals own and thus provide their bank accounts in exchange for some sort of financial reward, as the literature on money mule recruitment and involvement in traditional organized crime consistently shows (Aston et al. 2009; Bekkers et al. 2020; Bekkers and Leukfeldt 2022; Custers et al. 2019; de Boer et al. 2022; Europol 2021; Leukfeldt 2014; Madarie and Kruisbergen 2020; Roks et al. 2021). That is likely also the reason money mule recruiters tend to target individuals with low financial capabilities (Bekkers et al. 2020; Leukfeldt and Kleemans 2019). This aspect of the money mule subculture is present online as well, as promoting a luxury lifestyle was found to be the most prevalent cybercrime involvement mechanism on Instagram (Bekkers and Leukfeldt 2022). Recruiters show images of money, display large stacks or envelopes with euro bills and claim it is possible to earn fast and substantial amounts of money.

In addition to the normalization of money muling and the reverence shown towards a luxury lifestyle, a third explanation for the involvement of money mules in cybercrime is the use of neutralization techniques, i.e., the excuses used to justify deviant behavior (Maruna and Copes 2005; Sykes and Matza 1957). For years, neutralization techniques have been argued to be one of the key factors that relates to the onset and/or persistence of criminal behavior (Andrews and Bonta 2010; Gendreau et al. 1996; Maruna and Copes 2005; Maruna and Mann 2006; Sykes and Matza 1957). In the case of money mules, some stated that they were not aware of having committed a criminal offence or of having collaborated with criminals (Leukfeldt and Kleemans 2019). Others denied responsibility for their behavior or claimed the security measures adopted by victims should have been better (Arevalo 2015; Leukfeldt and Kleemans 2019). Recruiters on Instagram are also known to make use of neutralization techniques, stressing that participation is legal or risk-free; as in, for example, "WEEKLY and LEGAL then you've come to the right place" (see Bekkers and Leukfeldt 2022). While some money mules may be manipulated into handing over their bank accounts and unwittingly and/or unwillingly participating in a crime, justifications and excuses thus seem to contribute to their behavior.

Although money mules constitute a very heterogeneous group, youth form a particularly vulnerable target group, especially in online environments where it is relatively easy to reach them. One study surveyed 686 money mules involved in online fraud in Australia and found that the majority was aged 15 to 34 (Aston et al. 2009). Another study reports comparable results in the Netherlands, showing that Dutch money mules are mainly young adults between the ages of 18 and 22 (Oerlemans et al. 2016). It has been argued that the peak of activity for money mules is indeed reached in youth or adolescence, similar to the age-crime curve of more traditional forms of offending (Brunton-Smith and McCarthy 2016; Goldsmith and Wall 2022; Moffitt 1993; Palmieri et al. 2021).

Recruitment of money mules is thus done via both offline and online social ties (Bekkers and Leukfeldt 2022; Leukfeldt and Kleemans 2019). Currently, there is little insight into the online involvement

mechanisms. Considering the ongoing digitization of crime and criminal opportunities and the importance of money mules to cybercriminal networks, intervening in the online recruitment process might lead to significant reductions in the prevalence of cybercrime and cybercrime victimization. To be able to block online pathways into cybercrime, it is first necessary to gain insight into the extent to which young people are actually willing to interact with the different ads run by online recruiters.

3. Current study

Building on previous studies on offline and online cybercrime involvement mechanisms (Bekkers and Leukfeldt 2022; Leukfeldt and Kleemans 2019; Moneva et al. 2022), we developed two online ad campaigns for Instagram to reflect the *modus operandi* of criminals operating offline. The objective of these campaigns was to measure the engagement generated by three different money mule recruitment ads that reflect key cybercrime involvement mechanisms: promoting a luxury lifestyle, normalizing money muling, and applying neutralization techniques. These ads featured a call to action—a call to click on "Contact us"—that mirrors the efforts of real-life recruiters to establish contact with mules and obtain their bank account details. We used Facebook's Ads Manager Tool for both campaigns, to run both Instagram in-feed and Instagram Stories ads, and we targeted Dutch users aged 18 to 25. Instagram Feed is a mobile-first destination where users can share photos and videos, view shared or sponsored content, and connect with their community (Meta 2022a). Instagram Stories is an added feature that allows users to share or view shared or sponsored content for just 24 hours.

Because Facebook's Ads Manager Tool does not allow users to distribute ads randomly, we assigned Instagram users to mutually exclusive groups, in line with previous experimental studies on social media (Coppock et al. 2022; Jilke et al. 2019; Ryan 2012). How the ads are run depends on their metadata (e.g., popularity, time, and date of the post), the persons who created them (e.g., past interactions), and the preferences of the user, such as type of device, past activity and history of interactions (Meta 2022b; Mosseri 2021). Based on this, Instagram then determines how likely an individual is to engage with a post

and thus which ads will target which users each time they open Instagram. With this quasi-experimental 3 x 2 factorial design (i.e., three ads, two placements), we were able to compare the performance of each ad in each of the two campaigns. Specifically, we measured the reach and views of the ads, the number of accounts that clicked on the ads, the gender of the users who interacted with the ads, and the temporal distribution of reach and clicks per campaign.

4. Research design

The objective of the first campaign was to maximize the reach of the ads (i.e. the number of users seeing the ads, which corresponds to the objective identified as "reach"), while the objective of the second campaign was to maximize the interaction generated by the ads (i.e. the number of users that click on the ad, which corresponds to the objective identified as "traffic"). Specific settings and algorithms were optimized to reach the objective of each campaign. In the first campaign, users only saw the ads once, while in the second campaign there was no limit on the number of views per user. Users in the second campaign thus had the opportunity to click on the ads more often, thereby increasing the likelihood of engagement and of reaching the campaign objective. This set-up is similar to what happens with offline recruiters, as they ask money mules for their bank account multiple times before convincing them (Leukfeldt and Kleemans 2019). Also, the link in the ads on which users have to click corresponds to the strategy used by actual recruiters to prompt personal messages from money mules. We assume that the users that click on the link are interested in earning money with their bank cards and risk being money mules. Each combination of ad type and placement was linked to specific collections of Instagram users, thereby preventing overlapping respondents in the user groups. With these two experiments, we were able to examine the engagement of young users with the ads in different scenarios.

4.1. Ethics

Our research was approved by the Ethical Review Board of the Hague University of Applied Sciences. The ads themselves did not contain information about their actual purpose, because this would have obstructed our research. Instead, they redirected users to an external landing page to be debriefed by means of a disclaimer explaining that the ads were part of an awareness campaign and that no personal information had been collected or stored. Users exposed to the ads could choose whether to interact with them, so our sample was self-selected.

4.2. Users

Facebook's Ads Manager Tool did not enable us to target individual users in a random fashion. Instead, we had to randomize Instagram users within clusters, like previous studies on social media (Coppock et al. 2022; Jilke et al. 2019; Ryan 2012). This method uses the ads manager tool to target users based on mutually exclusive demographics, interests and/or online behavior. In our case, the target group comprised Instagram users between the ages of 18 and 25 living in certain ZIP codes in six municipalities in the Netherlands. We chose to include only ZIP codes with a relatively considerable number of residents, because small areas tend to have too few Instagram users for Facebook's Ads Manager Tool to estimate potential reach. The ZIP codes were then randomly assigned to the six user groups. Users could only see the ads linked to their specific ZIP code. Each user group was guaranteed a potential reach (i.e., the approximate number of Instagram users that can see the corresponding ads) of around 10,000 per user group of each campaign to ensure that each group would have enough participants for analysis, adding up to a total potential reach of 120,000 for the two campaigns combined. A total of 84 clusters of Instagram users were enough to accomplish said potential reach for each user group in each of the two campaigns.

4.3. The ads

The ads were designed according to those ads posted by actual money mule recruiters and the relevant literature. All three ads contained the same message, i.e., that individuals could earn money with their bank card. The ads also varied in terms of three central mechanisms that may explain why money mules become involved in cybercrime via social media: 1) promoting a *luxury lifestyle*, 2) *normalizing* money muling, and 3) applying *neutralization* techniques. These three mechanisms were represented in the ads by means of a single sentence. We have translated the original message from Dutch into English for the purposes of this article, which reflects the poor language used by recruiters in their ads. The ads were similar in length, appearance, and tone, and were run both on the Instagram Feed and Stories features separately to account for the effect of these two different placements. Luxury lifestyle and Feed functioned as control conditions since they appear to be used most frequently by actual recruiters.
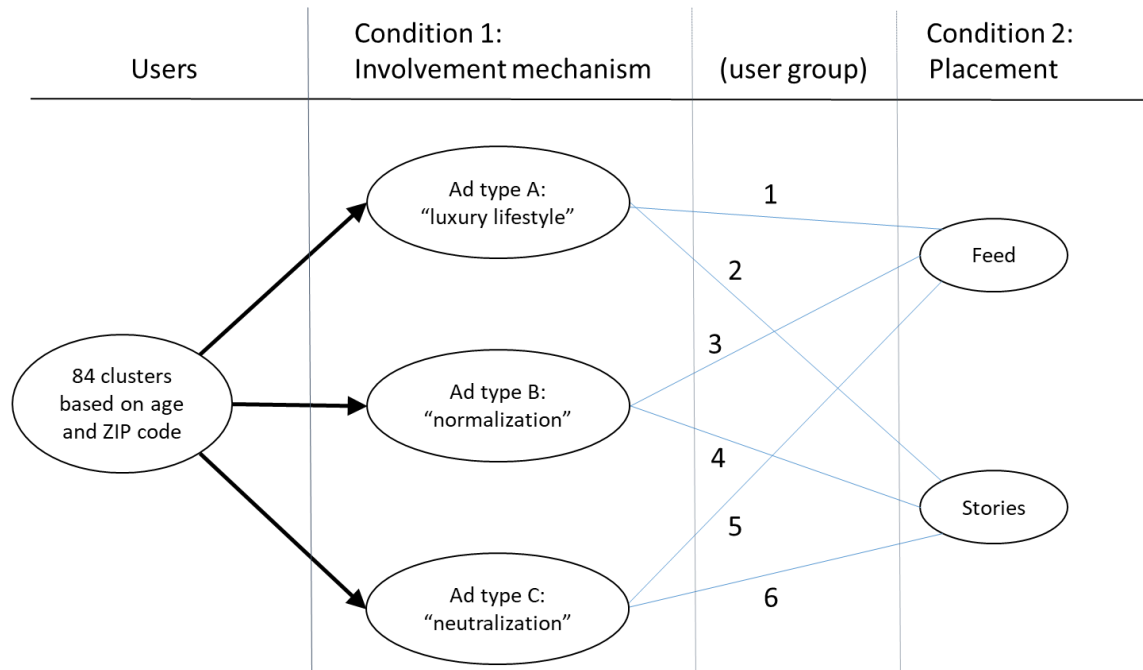
Table 1. Message of the ads

Involvement mechanism	Description
Luxury lifestyle	Earn money with your bankcard? Click here! 👇 You will soon have a few thousand !!
Normalization	Earn money with your bankcard? Click here! 👇 Others did it before you !!
Neutralization	Earn money with your bankcard? Click here! 👇 It is completely legal !!

Table 2. Overview of the experimental groups and conditions

User group	Involvement mechanism	Placement
1	Luxury lifestyle [c]	Feed [c]
2	Luxury lifestyle [c]	Stories
3	Normalization	Feed [c]
4	Normalization	Stories
5	Neutralization	Feed [c]
6	Neutralization	Stories

[c] control condition

Figure 1. Overview of the research design

| Users | Condition 1: Involvement mechanism | (user group) | Condition 2: Placement |

Ad type A: "luxury lifestyle"

84 clusters based on age and ZIP code

Ad type B: "normalization"

Ad type C: "neutralization"

1
2
3
4
5
6

Feed

Stories

4.4. Analytic strategy

We measured how many unique users the ads reached, their gender, how many times they saw the ads, how many times they clicked on them (i.e., engagement), when they did so and the click-through-rate (CTR) for each user group. Of the many metrics Instagram tracks, we used "Outbound Clicks" to determine the number of users responding to the call to act. This percentage indicates the number of individuals referred to destinations outside of Facebook. For the temporal distribution of user engagement per hour in the day, we used the measure "Unique Clicks (All);" Facebook claims to be unable to measure the Unique Outbound Clicks per hour, due to the amount of data processing that would require. We then conducted Chi-square tests of independence to compare the metrics of the groups.

It is worth mentioning that because of the heavy data processing required to calculate exact statistics, Instagram uses estimates (Meta 2022c). Facebook states that these estimates are highly accurate, as they are based on various sources, such as similar campaigns, users' interactions with ads and representative sampling. Of course, it is well known that clicks on ads can be attributed to bots or fake accounts rather

than actual human beings. To counter bot activity, Instagram has introduced additional measures to detect and block bots and fake profiles (Mosseri 2021).

Figure 2. Overview of the two campaigns
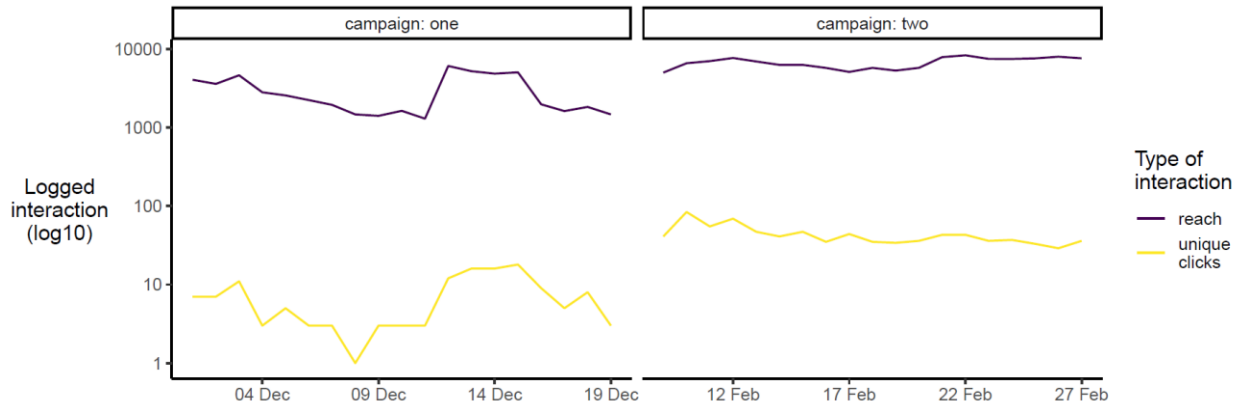
4.5. The campaigns

In both campaigns, the ads were first visible for 19 days, from 1 December 2021 to 19 December 2021 and then from 9 February 2022 to 27 February 2022 (Figure 2). Instagram estimated that a total of 92,963 unique users saw one of the ads of at least one of the campaigns. Of these accounts, 55,160 were linked to the first campaign, in which 136 unique users clicked on the "Contact us" button. Reach and clicks were strongly and positively correlated throughout the first campaign ($r(17) = 0.844$, $p < 0.001$). This campaign cost 1,684.21 Euros, which is the equivalent of approximately 0.03 Euros per user reached and 0.08 Euros per unique click. In the second campaign, the reach was much lower, but the clicks much higher: 37,803 and 770, respectively. These differences reflect the different objectives associated with the campaigns. In contrast to the first campaign, reach and clicks were not significantly correlated in the second campaign ($r(17) = 0.068$, $p = 0.781$). The costs of the second campaign amounted to 4,583.37 Euros, or 0.12 Euros per user reached and 5.95 Euros per click.

5. Results

The performance of the various ads is described in Table 3. In the first campaign, we found an overall CTR of 0.25%. More specifically, the luxury lifestyle ad is associated with the highest level of engagement (0.30%), followed by the neutralization ad (0.27%), and lastly by the normalization ad (0.16%). The difference in engagement between the luxury lifestyle and normalization ads is significant ($\chi^2(1) = 7.502$, $p < 0.05$), as is the difference between the neutralization and the normalization ads ($\chi^2(1) = 5.094$, $p < 0.05$). There are no significant differences between the luxury lifestyle and neutralization ads. In the second campaign, the overall click rate is 2.04%, which is higher than that of the first campaign. Once again, the luxury lifestyle and neutralization ads have a significantly higher click rate than the normalization ad (respectively, $\chi^2(1) = 16.838$, $p < 0.001$ and $\chi^2(1) = 9.078$, $p < 0.05$). The difference between the luxury lifestyle and neutralization ads is not significant. Therefore, the normalization mechanism appears to generate less engagement with youth than the luxury lifestyle and neutralization mechanisms. Furthermore, in both campaign rounds, the click rate of the ads featured on Stories was higher than in-feed ads. This difference is only significant in the second campaign ($\chi^2(1) = 13.994$, $p < 0.001$).

When zooming in on the specific user groups (Table 4, Table 5, Table 6, and Table 7), in the first campaign we found that the Stories luxury lifestyle ad had the highest level of engagement (0.38%), closely followed by the Stories neutralization ad (0.32%). By contrast, the normalization ad run on Stories (0.14%) and Feed (0.19%) was clicked on less often. In the first campaign, user group 2 differed significantly from group 3 ($\chi^2(1) = 5.692$, $p < 0.05$) and group 4 ($\chi^2(1) = 10.865$, $p < 0.01$), while user group 4 also differed from group 6 ($\chi^2(1) = 6.929$, $p < 0.05$). In the second campaign, the luxury lifestyle ad featured on Stories had the highest level of engagement (2.93%), followed by the neutralization ad run on Feed (2.24%). The in-feed normalization ad was clicked on less frequently (1.24%). Herein we see that

the highest and lowest scoring user groups (group 2 and 3 respectively) differ significantly from all other groups. No other differences were significant.

Table 3. Ad performance

	Reach	**Views**	**Clicks**	**CTR**	
Ad type					
Campaign 1					
Luxury	17,944	18,246	54	0.0030	(0.30%)
lifestyle	18,904	19,212	31	0.0016	(0.16%)
Normalization	18,312	18,660	51	0.0027	(0.27%)
Neutralization					
Campaign 2					
Luxury	11,819	48,853	279	0.0236	(2.36%)
lifestyle	12,757	56,063	208	0.0163	(1.63%)
Normalization	13,227	56,651	283	0.0214	(2.14%)
Neutralization					
Placement					
Campaign 1					
Stories	27,651	27,875	76	0.0028	(0.28%)
Feed	27,509	28,243	60	0.0021	(0.21%)
Campaign 2					
Stories	19,375	91,131	446	0.0230	(2.30%)
Feed	18,428	70,436	324	0.0176	(1.76%)
Total					
Campaign 1	55,160	56,118	136	0.0025	(0.25%)
Campaign 2	37,803	161,567	770	0.0204	(2.04%)

Table 4. Reach and clicks per user group. Campaign 1

User group	**Reach**	**Views**	**Clicks**	**CTR**	
1	9,300	9,529	21	0.0023	(0.23%)
2	8,644	8,717	33	0.0038	(0.38%)
3	9,350	9,599	18	0.0019	(0.19%)
4	9,554	9,613	13	0.0014	(0.14%)
5	8,859	9,115	21	0.0023	(0.23%)
6	9,453	9,545	30	0.0032	(0.32%)

Table 5. Comparison of CTR of user groups (Chi-square tests of independence). Campaign 1

Involvement mechanism	1	2	3	4	5	6
(1) Luxury lifestyle on Feed	-					
(2) Luxury lifestyle on Stories	3.632	-				
(3) Normalization on Feed	0.248	5.692*	-			
(4) Normalization on Stories	2.108	10.865**	0.920	-		
(5) Neutralization on Feed	0.025	2.979	0.422	2.543	-	
(6) Neutralization on Stories	1.449	0.540	2.877	6.919*	1.062	-

* = p < 0.05. ** = p < 0.001

Table 6. Reach and clicks per user group. Campaign 2

User group	Reach	Views	Clicks	CTR	
1	5,616	20,915	97	0.0173	(1.73%)
2	6,203	27,938	182	0.0293	(2.93%)
3	6,033	23,725	75	0.0124	(1.24%)
4	6,724	32,338	133	0.0198	(1.98%)
5	6,779	25,796	152	0.0224	(2.24%)
6	6,448	30,855	131	0.0203	(2.03%)

Table 7. Comparison of CTR of user groups (Chi-square tests of independence). Campaign 2

Involvement mechanism	1	2	3	4	5	6
(1) Luxury lifestyle on Feed	-					
(2) Luxury lifestyle on Stories	18.626**	-				
(3) Normalization on Feed	4.685*	42.526**	-			
(4) Normalization on Stories	1.052	12.406**	10.706*	-		
(5) Neutralization on Feed	4.138	6.185*	18.307**	1.141	-	
(6) Neutralization on Stories	1.500	10.671*	11.937**	0.048	0.700	-

* = p < 0.05. ** = p < 0.001

We also examined the relationship between the gender of our participants and their interaction with the ads. Figure 3 indicates that the first campaign had more female participants, while the majority of the second campaign consisted of males. It is noted females may use social media more often (Statistics Netherlands 2021; Su et al. 2020), thereby explaining the higher number of females in the first campaign, while the algorithms of Instagram possibly identify male users as generally more likely to engage with the ads (see also Arevalo 2015; Aston et al. 2009; Bekkers et al. 2020; Oerlemans et al. 2016), which can explain the prevalence of male users in the second campaign. The latter notion is confirmed by the data,

as in both rounds, males were significantly more likely to engage with the ads than females ($\chi^2(1) = 26.382$, $p < 0.001$; $\chi^2(1) = 87.724$, $p < 0.001$).

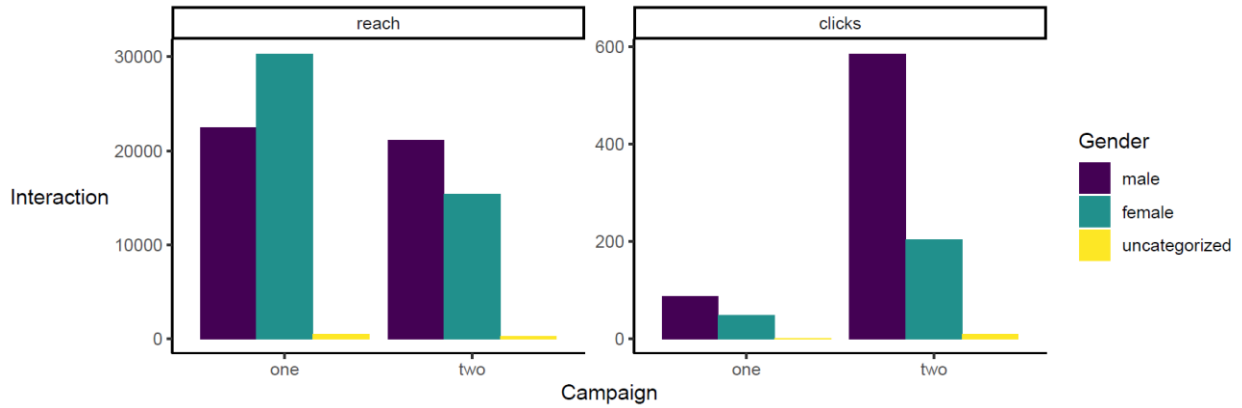*Figure 3. Gender distribution by type of interaction per campaign*

Figure 4a shows the temporal distribution of the reach and clicks of the ads per hour in the day. Note that in the first campaign most users engaged with the ads in the morning, in the slot between 07:00 and 10:00 am, with a slight peak in the afternoon and early evening. There are no notable differences between the trend in reach and clicks in this case. The second campaign shows a somewhat different curve, where the reach and number of clicks is more distributed over the day. In both rounds, the absolute numbers of reach and clicks seem to follow the routine activities of youth, as they are more active on social media during the day. However, these patterns change in Figure 4b, which depicts the CTR. In the first campaign, there are some peaks in engagement during the day; but, in both campaigns, there is considerable engagement at night (from around 00:00 to 06:00 am). Given that it is unusual for users to click on ads in this time slot, the results suggest that there is a small group of them purposely looking for ways to earn money.

Figure 4. Time patterns of interaction per campaign: a) reach and total clicks; b) CTR
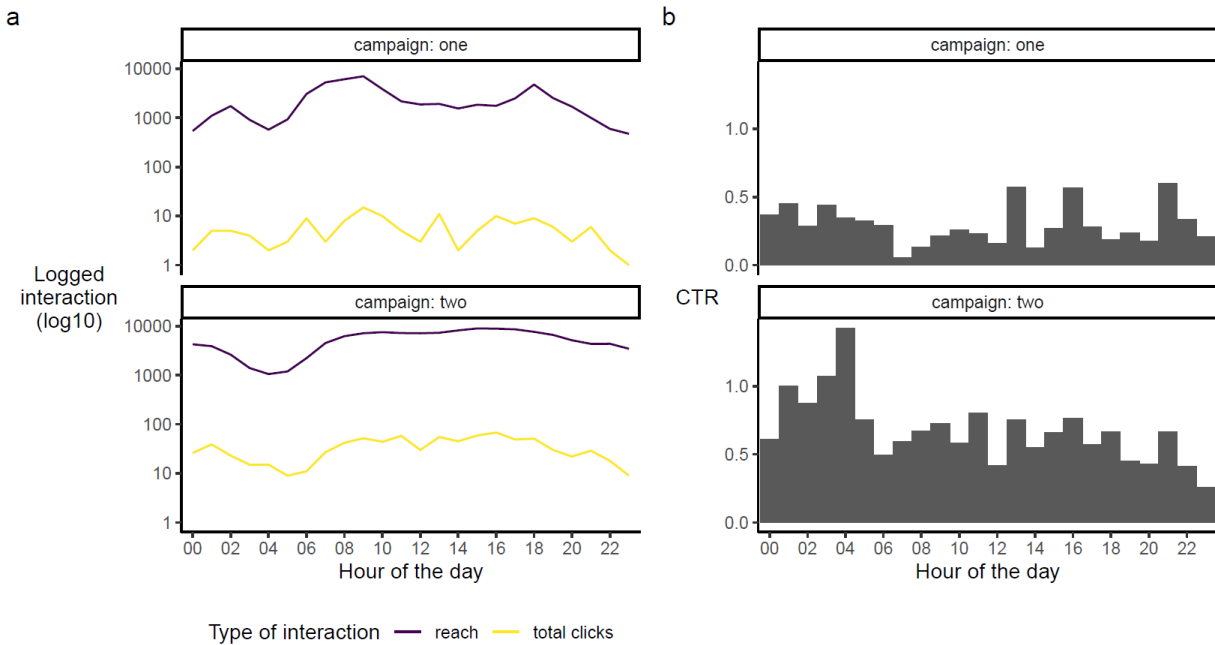
6. Discussion

For the purposes of this study, we carried out two field experiments on Instagram. The goal of these experiments was to test the level of engagement of young users with ads aimed at recruiting money mules, in order to understand the online involvement mechanisms of cybercrime. With the use of the Facebook Ads Manager, we ran three different ads in two Instagram placements, which resulted in a quasi-experimental 3 x 2 factorial design. The message of the ads revolved around making money with bank cards and each one utilized a different cybercrime involvement mechanism, thus mirroring the online environment of money mule recruitment on Instagram (Bekkers and Leukfeldt 2022). As conducting experiments on Instagram does not allow individual users to be randomized for experimental conditions, we followed the recommendations of previous experimental research and created 84 clusters of Dutch Instagram users based on age and ZIP code; we then randomized said clusters according to the different conditions of the two campaigns (Broockman and Green 2014; Jilke et al. 2019; Ryan 2012). Although experimenting with ads on social media is quite innovative in the case of criminological studies

(e.g., Moneva et al. 2022), it is a well-known approach in other fields, such as political science and marketing (e.g., Bakshy et al. 2012; Broockman and Green 2014; Coppock et al. 2022).

One aspect worth mentioning is that when experiments are conducted on Instagram there is a lack of transparency on how and when ads are shown to users, as the algorithms of Instagram can lead to selection bias. Indeed, the algorithms learn which users are most likely to engage with these types of ads, so the ads tend to be shown to those exact users to meet the associated campaign objective. As a result, the probability of individual users being exposed to the ads may very well differ per experimental condition. We addressed this issue by opting for cluster randomization and re-creating the actual environment in which money mules are recruited. Also, all users across all conditions are subject to the same algorithms. The experiment is therefore still valid (e.g., Gordon et al. 2019). A second consideration is that there is no information available regarding the motives behind clicks. Hence, we cannot tell if users were actually willing to provide their bank account information or if they had other reasons for engaging with the ads. We encourage future researchers to conduct similar experiments in more controlled settings, so that they can follow up with the individuals exposed to the ads. This is not only necessary to better comprehend the reasons behind their engagement, but also because with the current set-up it is not known to what extent money mule advertising campaigns could actually lead to prevention. Evaluating the effectiveness of online crime prevention strategies is a difficult but essential line of research to tackle money muling. A third issue is that Facebook cannot produce actual figures on user interaction with ads: it can only provide estimates due to the heavy data processing needed for hard data elaboration (Meta 2022c). The exact number of young people that engaged with the ads is therefore not known. Also, for the same reasons, it was not possible for Facebook to calculate the outbound clicks per hour in the day. In this case, we were forced to use a different but less accurate measure, namely all unique clicks.

The two experiments showed that advertising on Instagram is a promising way to reach the target group. In just over a month, a total of nearly 100,000 different Instagram accounts saw one of the ads meant to

recruit money mules and 906 of these accounts engaged with the call to action (i.e., "Contact us"). This suggests that about 1% of young users on Instagram are interested in earning money with their bank card. If we zoom in on the user groups, the CTR for each group varied between 0.14% and 0.38% in the first campaign, and between 1.24% and 2.93% in the second campaign. As the differences in CTR imply, the results were highly dependent on the specific message in the ads and the associated campaign objective. The first campaign was aimed at maximizing exposure and reached 55,160 accounts, 136 of which clicked on one of the ads (with an overall CTR of 0.25%). The second campaign was aimed at maximizing engagement and in the same number of days reached 37,803 accounts, of which 770 clicked on one of the ads (with an overall CTR of 2.04%). Therefore, the differences in ad performance across the two campaigns reflect the objectives that were set beforehand, as they were associated with specific algorithms that are optimized to reach the objective. Also, users saw the ads multiple times in the second campaign, as opposed to the first, which increases their chances of interacting. Therefore, more frequent requests from recruiters may convince users to become involved in cybercrime (Leukfeldt and Kleemans 2019).

Regarding the message of the ads, we observed that in both campaigns advertising a luxury lifestyle (i.e., "earn fast and lots of money") or using neutralization techniques (i.e., "earn money legally") lead to significantly more clicks than normalizing the activity of money muling (i.e., "others have done it before you"). This confirms the results of previous research, namely that some users are indeed keen to make "a quick buck" and that this is a primary motivation for money mules recruited both online and offline (Bekkers and Leukfeldt 2022; Leukfeldt and Kleemans 2019; Roks et al. 2021). At the same time, young Instagram users also seem vulnerable to manipulation, as statements about making money legally work well as a persuasion strategy. This indicates that youth may have limited knowledge about the phenomenon of money muling. However, the use of neutralization techniques by real recruitment accounts is rare (Bekkers and Leukfeldt 2022). This may be explained by the notion that actual recruiters already have an established network of young people who are familiar with this illegal activity and who

have perhaps even acted as money mules in the past, contrary to the general Instagram audience who was exposed to our ads. This may also explain why the normalization of money muling worked less well in our study: the general youth population still does not consider it acceptable to engage in potentially fraudulent activities.

These results raise questions about the generalizability of the results to young users outside the Netherlands. While it is likely that social media platforms like Instagram are also used in other countries to reach potential money mules, and similar techniques employed by recruiters to attract users (Europol 2021; Federal Bureau of Investigation 2022; Hutchings and Holt 2015), additional comparative research is required to understand the online involvement mechanisms of cybercrime in other countries, and the similarities and differences in the activity of locally oriented criminal networks. The knowledge in this area is limited because much of the literature on money mule recruitment focuses on case studies (e.g., Bekkers and Leukfeldt 2022; Leukfeldt and Kleemans 2019; Roks et al. 2021).

The ads targeted users via two different Instagram placements, namely users' Feeds and Stories, the purpose being to account for the effect of these placements on the level of users' engagement. The reach of the ads in said placements appeared to be comparable, but Stories ads were shown more often to the same users, meaning users had more opportunities to click on them. This might explain the higher CTR for Stories ads compared to in-feed ads. Furthermore, it appears that men are more likely to interact with our ads than women, as confirmed by the literature, which implies that young males are especially susceptible to becoming involved in cybercrime (Arevalo 2015; Aston et al. 2009; Bekkers et al. 2020; Holt 2020; Moneva et al. 2022; Oerlemans et al. 2016). It is also worth noting that users clicked on the ads more often during the day—that is, in absolute numbers—but the percentage of those who clicked seemed higher at night. It is likely that most young users click on an ad opportunistically whilst checking their social media accounts as part of their routine, but that a small segment of users also perform

21

purposeful searches, looking for ways to earn money, at odd hours at night (see also Moneva et al. 2022). This group might be particularly vulnerable to becoming involved in cybercrime.

Our findings also have some practical implications, as they can be used in the context of an intervention focused on money mules in the light of situational crime prevention. Defined as a pragmatic approach rather than a theoretical framework, situational crime prevention seeks to reduce opportunities for crime (Clarke 1980, 2017; Cornish and Clarke 2003). The focus is to alter criminal behavior by creating a situation in which it is no longer desirable to commit such acts. To be effective, situational crime prevention must be crime-specific, i.e., its techniques should be focused on specific forms of criminal behavior. In this regard, Instagram seems to be a promising and cost-effective way to reach youth at risk of becoming money mules to disrupt the online socialization process that leads to their involvement in cybercrime. The ads are relatively easy to deploy and require only a basic knowledge of how Instagram and the Facebook Ads Manager tools work. If the goal of the intervention is to maximize the exposure of youth to ads, then we recommend opting for informative ads. On the other hand, ads on Instagram can also be used to refer the target group to destinations outside of Instagram to ensure more extensive behavioral intervention. The latter is usually a more expensive way of advertising, as shown in this study.

Within the situational crime prevention framework, reducing provocations that incite criminal behavior and removing excuses for the behavior (see Cornish and Clarke 2003) might be particularly valuable in the case of online money mule recruitment. For instance, our findings suggest that youth have a lack of knowledge about being a money mule and the risks associated with it, while money mules have a high likelihood of detection and can face severe consequences at a later age. Thus, raising awareness among the target group may be a useful mechanism to remove excuses for money muling, informing for instance about the illegal nature of money muling and the impact of cybercrime on its victims. Moreover, because it seems that young people are more inclined to engage with ads claiming they can earn fast and lots of money, it may be that they are prompted to do so due to a lack of financial means or the absence of

22

legitimate work (Bekkers and Leukfeldt 2022; Leukfeldt and Kleemans 2019). To reduce such

provocations, at-risk youth must have access to resources that can help them find honest work, or to

organizations that offer assistance with debt. Instagram can be used to reach those users and to refer them

to the support they need. This might be a particularly valuable strategy, since there is evidence that

interventions based on therapeutic approaches (e.g., counseling, rehabilitation, offering guidance) may be

more effective than those that use deterrence and sanctioning (Lipsey and Cullen 2007; Wormith et al.

2007).

Acknowledgements

References

Andrews, D. A., & Bonta, J. (2010). Rehabilitating criminal justice policy and practice. *Psychology, Public Policy, and Law*, *16*(1), 39–55. https://doi.org/10.1037/a0018362

Arevalo, B. C. (2015). *Money Mules: Facilitators of financial crime. An explorative research on money mules* (Master's Thesis). Utrecht University. Retrieved from https://d1wqtxts1xzle7.cloudfront.net/49127520/Money_Mule_Thesis_Brenda_Arevalo-with-cover-page-v2.pdf?Expires=1665745550&Signature=EsQ0x632iqoG7VwgeZrTdmqESLWw1LGOkZljS0bZ28ATTSrXjPSoCogrsd~u~B9wi26nRUmjjPoN7vQv1rdgxFhUSFs1Q2CigbhwCPm3H5nZ-lNIJFJzZSy7dg-Unbom~Qa7j9PQTTl2SUwqTD6zS2cfm69OI~UkXCeeL4tIoEQch2cIZXxyGtsuZqujHQ5R8N-4kdNYZZZaRjfSBXYksUXKFHrfCVe0UcqUl97uWRKBgdq-jSqbDGbRFz1GZZTDldlbsat6nuT76T4u0I2rF-2MoYmcDMaUw~vnKKKB3yTMt3aDXUx07mwSP0Z~fht8mFtH1A~5QxKCoa6Pvuu4SA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

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* (pp. 482–487). Presented at the 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, Brisbane, Australia: IEEE. https://doi.org/10.1109/UIC-ATC.2009.63

Bakshy, E., Eckles, D., Yan, R., & Rosenn, I. (2012). Social influence in social advertising: evidence from field experiments. In *Proceedings of the 13th ACM Conference on Electronic Commerce - EC '12* (p. 146). Presented at the the 13th ACM Conference, Valencia, Spain: ACM Press. https://doi.org/10.1145/2229012.2229027

Bekkers, L. M. J., & Leukfeldt, E. R. (2022). Recruiting money mules on Instagram: a qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior*, 1–17. https://doi.org/10.1080/01639625.2022.2073298

Bekkers, L. M. J., Schiks, J. A. M., & Leukfeldt, E. R. (2020). *Naar een interventie tegen geldezels. Een pilot in de gemeente Haarlem* (pp. 1–24). The Hague University of Applied Sciences. https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/expertisecentra/naar-een-interventie-tegen-geldezels_een-pilot-in-de-gemeente-haarlem.pdf?sfvrsn=930f4c56_2

Brake, M. (2013). *Sociology of Youth Culture and Youth Subcultures (Routledge Revivals): Sex and Drugs and Rock "n" Roll*.

Broockman, D. E., & Green, D. P. (2014). Do Online Advertisements Increase Political Candidates' Name Recognition or Favorability? Evidence from Randomized Field Experiments. *Political Behavior*, *36*(2), 263–289. https://doi.org/10.1007/s11109-013-9239-z

Brunton-Smith, I., & McCarthy, D. J. (2016). Explaining Young People's Involvement in Online Piracy: An Empirical Assessment Using the Offending Crime and Justice Survey in England and Wales. *Victims & Offenders*, *11*(4), 509–533. https://doi.org/10.1080/15564886.2015.1121943

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., de Poot, C., et al. (2016). *Cyber-OC – Scope and manifestations in selected EU member states* (No. 50) (pp. 1–298). Bundeskriminalamt Criminalistic Institute. https://eucpn.org/sites/default/files/document/files/52._cyber-oc_-_scope_and_manifestations_in_selected_eu_member_states.pdf

Calderoni, F., Campedelli, G. M., Communale, T., Marchesi, M., & Savona, E. (2020). *Recruitment into organised criminal groups: A systematic review*. Australian Institute of Criminology. https://doi.org/10.52922/ti04183

Calderoni, F., Campedelli, G. M., Szekely, A., Paolucci, M., & Andrighetto, G. (2022). Recruitment into Organized Crime: An Agent-Based Approach Testing the Impact of Different Policies. *Journal of Quantitative Criminology*, *38*(1), 197–237. https://doi.org/10.1007/s10940-020-09489-z

Campedelli, G. M., Calderoni, F., Comunale, T., & Meneghini, C. (2021). Life-Course Criminal Trajectories of Mafia Members. *Crime & Delinquency*, *67*(1), 111–141. https://doi.org/10.1177/0011128719860834

Clarke, R. V. (1980). "Situational" Crime Prevention: Theory and practice. *The British Journal of Criminology*, *20*(2), 136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Clarke, R. V. (2017). Situational crime prevention. In R. Wortley & M. Townsley (Eds.), *Environmental Criminology and Crime Analysis* (2nd ed., pp. 1–25). London, UK; New York, NY: Routledge, Taylor & Francis Group.

Coppock, A., Green, D. P., & Porter, E. (2022). Does digital advertising affect vote choice? Evidence from a randomized field experiment. *Research & Politics*, *9*(1), 205316802210769. https://doi.org/10.1177/20531680221076901

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley´s critique of situational crime prevention. In M. J. Smith & D. B. Cornish (Eds.), *Theory for practice in situational crime prevention* (pp. 41–96). New York, NY: Criminal Justice.

Custers, B. H. M., Pool, R. L. D., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. *European Journal of Criminology*, *16*(6), 728–745. https://doi.org/10.1177/1477370818788007

de Boer, H., Ferwerda, H., & Kuppens, J. (2022). *Do or Don't. Kennissynthese ingroeimechanismen en rekruteringsprocessen van jongeren in de georganiseerde criminaliteit* (pp. 1–69). Ministerie van Justitie en Veiligheid, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). https://repository.wodc.nl/bitstream/handle/20.500.12832/3154/3203-do-or-don%27t-volledige-tekst.pdf

Dunham, K. (2006). Money Mules: An Investigative View. *Information Systems Security*, *15*(1), 6–10. https://doi.org/10.1201/1086.1065898X/45926.15.1.20060301/92679.2

Europol. (2021). Money Muling. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling

Federal Bureau of Investigation. (2022). Money Mules. *How We Can Help You*. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/money-mules

Felson, M. (2003). The Process of Co-offending. *Crime Prevention Studies*, *16*, 149–167.

Gendreau, P., Little, T., & Goggin, C. (1996). A Meta-analysis Of The Predictors Of Adult Offender Recidivism: What Works! *Criminology*, *34*(4), 575–608. https://doi.org/10.1111/j.1745-9125.1996.tb01220.x

Goldsmith, A., & Wall, D. S. (2022). The seductions of cybercrime: Adolescence and the thrills of digital transgression. *European Journal of Criminology*, *19*(1), 98–117. https://doi.org/10.1177/1477370819887305

Gordon, B. R., Zettelmeyer, F., Bhargava, N., & Chapsky, D. (2019). A Comparison of Approaches to Advertising Measurement: Evidence from Big Field Experiments at Facebook. *Marketing Science*, *38*(2), 193–225. https://doi.org/10.1287/mksc.2018.1135

Herbert, S. (1998). Police Subculture Reconsidered. *Criminology*, *36*(2), 343–370. https://doi.org/10.1111/j.1745-9125.1998.tb01251.x

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198. https://doi.org/10.1080/01639620601131065

Holt, T. J. (2020). Computer Hacking and the Hacker Subculture. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 725–742). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_31

Hutchings, A., & Holt, T. J. (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

Ianni, F. A. J., & Reuss-Ianni, E. (1972). *A family business: kinship and social control in organized crime*. New York: Russell Sage Foundation.

Jilke, S., Lu, J., Xu, C., & Shinohara, S. (2019). Using Large-Scale Social Media Experiments in Public Administration: Assessing Charitable Consequences of Government Funding of Nonprofits. *Journal of Public Administration Research and Theory*, *29*(4), 627–639. https://doi.org/10.1093/jopart/muy021

Kleemans, E. R., & de Poot, C. J. (2008). Criminal Careers in Organized Crime and Social Opportunity Structure. *European Journal of Criminology*, *5*(1), 69–98. https://doi.org/10.1177/1477370807084225

Kleemans, E. R., & van Koppen, V. (2020). Organized Crime and Criminal Careers. *Crime and Justice*, *49*, 385–423. https://doi.org/10.1086/707318

Leukfeldt, E. R. (2014). Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555. https://doi.org/10.1089/cyber.2014.0008

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*, 106979. https://doi.org/10.1016/j.chb.2021.106979

Leukfeldt, E. R., & Kleemans, E. R. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In S. Hufnagel & A. Moiseienko (Eds.), *Criminal networks and law enforcement: global perspectives on illegal enterprise* (pp. 75–89). London ; New York: Routledge, Taylor & Francis Group. https://research.vu.nl/ws/portalfiles/portal/85076479/Cybercrime_money_mules_and_situational_crime_prevention.pdf

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology*, *57*(3), 704–722. https://doi.org/10.1093/bjc/azw009

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39–53. https://doi.org/10.1007/s10611-016-9663-1

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017c). 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

Lipsey, M. W., & Cullen, F. T. (2007). The Effectiveness of Correctional Rehabilitation: A Review of Systematic Reviews. *Annual Review of Law and Social Science*, *3*(1), 297–320. https://doi.org/10.1146/annurev.lawsocsci.3.081806.112833

Madarie, R., & Kruisbergen, E. W. (2020). Traffickers in Transit: Analysing the Logistics and Involvement Mechanisms of Organised Crime at Logistical Nodes in the Netherlands: Empirical Results of the Dutch Organised Crime Monitor. In D. Weisburd, E. U. Savona, B. Hasisi, & F. Calderoni (Eds.), *Understanding Recruitment to Organized Crime and Terrorism* (pp. 277–308). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-36639-1_12

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*(1), 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

Maruna, S., & Copes, H. (2005). What Have We Learned from Five Decades of Neutralization Research? *Crime and Justice*, *32*, 221–320. https://doi.org/10.1086/655355

Maruna, S., & Mann, R. E. (2006). A fundamental attribution error? Rethinking cognitive distortions†. *Legal and Criminological Psychology*, *11*(2), 155–177. https://doi.org/10.1348/135532506X114608

Meta. (2022a). Help Center. *Help Center*. https://help.instagram.com/

Meta. (2022b). How Facebook Distributes Content. *Meta Business Help Center*. https://www.facebook.com/business/help/718033381901819?id=208060977200861

Meta. (2022c). About estimated, in-development metrics and third-party metrics. *Meta Business Help Center*. https://www.facebook.com/business/help/181058782494426#estimated

Moffitt, Terrie. E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: a developmental taxonomy. *Psychological Review*, *100*(4), 674–701.

Moneva, A., Leukfeldt, E. R., & Klijnsoon, W. (2022). Alerting consciences to reduce cybercrime: a quasi-experimental design using warning banners. *Journal of Experimental Criminology*. https://doi.org/10.1007/s11292-022-09504-2

Morselli, C. (2005). *Contacts, opportunities, and criminal enterprise*. Toronto ; Buffalo: University of Toronto Press.

Mosseri, A. (2021). Shedding More Light on How Instagram Works. *Instagram Blog*. https://about.instagram.com/blog/announcements/shedding-more-light-on-how-instagram-works

Moule, R. K., Pyrooz, D. C., & Decker, S. H. (2013). From 'What the F#@% is a Facebook?' to 'Who Doesn't Use Facebook?': The role of criminal lifestyles in the adoption and use of the Internet. *Social Science Research*, *42*(6), 1411–1421. https://doi.org/10.1016/j.ssresearch.2013.06.008

Oerlemans, J.-J., Custers, B. H. M., Pool, R. L. D., & Cornelisse, R. (2016). *Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Den Haag, Meppel: Boom criminologie ; Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), Ministerie van Veiligheid en Justitie ; Boom juridisch distributiecentrum.

Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior*, *120*, 106745. https://doi.org/10.1016/j.chb.2021.106745

Paoli, L. (2003). *Mafia brotherhoods: organized crime, Italian style*. Oxford ; New York: Oxford University Press.

Poushter, J., Bishop, C., & Chwe, H. (2018). *Social media use continues to rise in developing countries but plateaus across developed ones* (pp. 1–46). Pew Research Center.

https://www.pewglobal.org/wp-content/uploads/sites/2/2018/06/Pew-Research-Center_Global-Tech-Social-Media-Use_2018.06.19.pdf

Pratt, T. C., Cullen, F. T., Sellers, C. S., Thomas Winfree, L., Madensen, T. D., Daigle, L. E., et al. (2010). The Empirical Status of Social Learning Theory: A Meta-Analysis. *Justice Quarterly*, *27*(6), 765–802. https://doi.org/10.1080/07418820903379610

Quinn, J. F., & Forsyth, C. J. (2005). describing sexual behavior in the era of the internet: a typology for empirical research. *Deviant Behavior*, *26*(3), 191–207. https://doi.org/10.1080/01639620590888285

Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2021). The Hybridization of Street Offending in the Netherlands. *The British Journal of Criminology*, *61*(4), 926–945. https://doi.org/10.1093/bjc/azaa091

Ryan, T. J. (2012). What Makes Us Click? Demonstrating Incentives for Angry Discourse with Digital-Age Field Experiments. *The Journal of Politics*, *74*(4), 1138–1152. https://doi.org/10.1017/S0022381612000540

Statistics Netherlands. (2021). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte, 2020. *CBS StatLine*. https://opendata.cbs.nl/

Su, W., Han, X., Yu, H., Wu, Y., & Potenza, M. N. (2020). Do men become addicted to internet gaming and women to social media? A meta-analysis examining gender-related differences in specific internet addiction. *Computers in Human Behavior*, *113*, 106480. https://doi.org/10.1016/j.chb.2020.106480

Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. *American Sociological Review*, *22*(6), 664. https://doi.org/10.2307/2089195

van Dijk, M., Kleemans, E. R., & Eichelsheim, V. I. (2019). Children of Organized Crime Offenders: Like Father, Like Child? An Explorative and Qualitative Study Into Mechanisms of Intergenerational (Dis)Continuity in Organized Crime Families. *European Journal on Criminal Policy and Research*, *25*(4), 345–363. https://doi.org/10.1007/s10610-018-9381-6

van Koppen, M. V. (2013). Involvement mechanisms for organized crime. *Crime, Law and Social Change*, *59*(1), 1–20. https://doi.org/10.1007/s10611-012-9396-8

Wormith, J. S., Althouse, R., Simpson, M., Reitzel, L. R., Fagan, T. J., & Morgan, R. D. (2007). The Rehabilitation and Reintegration of Offenders: The Current Landscape and Some Future Directions for Correctional Psychology. *Criminal Justice and Behavior*, *34*(7), 879–892. https://doi.org/10.1177/0093854807301552