Profiling HMRC and IRS Scammers by Utilising Trolling Videos: The Scam Script

Abstract

Both the HM Revenue and Customs (HMRC) and the Internal Revenue Service (IRS) have issued public warnings regarding the increasing rates of scams targeting taxpayers and the high financial loss to governmental bodies and individuals around the globe these scams impact (HMRC, 2020a: IRS, 2021). However, despite this large impact on the economy, there is limited research on the working practices of the individuals behind these acts of fraud (Tzani-Pepelasi et al, 2020). The present study utilised videos where Internet trolls engage with HMRC/IRS scammers, who attempted to delay scammers and protect victims, to investigate the stages involved with this scam using crime script analysis. The findings of this study potentially highlight that such fraudulent operations utilise scam scripts with amendable steps, according to the scammers' experience and the victims' gullibility. The limitations and implications of the study are discussed.

Key words: Scams; IRS; HMRC; Taxpayers; Organised Crime.

Introduction

Fraudsters have always been trying to victimise consumers in order to profit (Age UK, 2015) by using a number of deceitful strategies to scam individuals and businesses out of hard-earned money and other objects of value. The technological advances of recent years have seen the opportunities and mechanisms for perpetrating fraud proliferate. Early in 2019, HM Revenue and Customs (HMRC) published a press release, warning households to be vigilant of phone calls from fraudsters pretending to be from the financial tax authority (HMRC, 2019). Similarly, in a press release from the Internal Revenue Service (IRS), American taxpayers were likewise cautioned to be alert for phone scams at tax time (March to May). During this period, fraudsters pose as IRS agents in the hope of stealing tax-payers' money or personal information (IRS, 2019).

Defining Fraud

Although, there have been numerous definitions of fraud or scams, the Office for National Statistics (2016), explains scams as misleading or deceptive business practices, in which individuals receive an unsolicited or uninvited contact (e.g., by email, letter, phone call or advertisement), involving false promises by the fraudsters, who aim to lure victims into paying money or other valuable objects. Tax phone scams are one type of such fraudulent operations that harm the public (Gorden & Buchanan, 2013). As well as the severe financial losses incurred, victims may also suffer emotionally from mental health problems, loss of employment, family disintegration and self-blame (Button, Lewis & Tapley, 2009). Despite numerous warnings and statements issued about these scams from the HMRC and the IRS, people are still reacting and replying to these attempts by the scammers to reach out to them. This potentially highlights

failings in the attempts by these tax branches to inform their customers on what they should be aware of when discussing tax issues over the phone or online, or perhaps customers are simply overlooking the warning signs exhibited by the scammers. Whilst fraud watch organisations regularly release reports of warning signs to look out for when being contacted by potentially fraudulent means (e.g., HMRC, 2019; IRS, 2018), scams still proliferate, and there is a lack of data and available research to determine how fraudsters continue to be successful. Acting upon this research gap and the necessity for further investigation, this paper examines the crime script used by scammers who impersonate government officials from the HMRC and the IRS to scam taxpayers.

Tax Scams and their Financial Impact

The HMRC and IRS scams are common types of impersonation scams from purported government agencies, in which perpetrators claim to represent an organisation such as a government department (Action Fraud, n.d); sending out official-looking letters and emails or making phone calls advising that you must pay a fee to comply with certain legislation, pay a fine for breaches of the law, or give bank details to claim a tax rebate or refund (Action Fraud, 2018; "Bogus government agency scams", n.d.; UK Finance, 2019). These scams are mostly based on a technique called phishing, sending e-mails or making phone calls that appear to be from reputable sources with the goal of gaining personal and financial information. That information is then stored in a database, which is used to scam taxpayers into giving large amounts of money (Banoff & Lipton, 2005; Hadnagy, Fincher & Dreeke, 2015; Kaniuk, 2016). Frequently, the scammers use an application called spoofing, with which they manage to replicate authentic governmental contact numbers. Therefore, the victims are persuaded that the call is legitimate. Thereafter, the payment takes place through various money transfer

mechanisms, such as wiring money directly through Western Union or MoneyGram (Federal Trade Commission, 2014).

Tax phone scams have generated particular concern in the last few years across the globe, with both the IRS in the USA and HMRC in the UK reporting staggering increases in impersonation or government agency scams, especially during tax filing seasons, which usually fall in the first part of the year (HMRC, 2019; IRS, 2018). In 2018, UK Finance published a report on data collected on reported fraud during that year. They found that impersonation scams constituted over 5,000 of the scams reported to UK Finance, with a total of £36.2 million in both personal and non-personal losses (UK Finance, 2019). Other organisations, such as Cifas and Action Fraud publish their data as part of the Office for National Statistics (ONS) regular crime bulletin (ONS, 2019).

Like the HMRC in the UK, tax-related identity theft and IRS impersonation telephone scams continue to cause a strain upon limited resources at the IRS and Treasury Inspector General for Tax Administration (TIGTA), challenging the integrity of the Federal tax administration in the USA. The TIGTA semi-annual report (TIGTA, 2018) for September 2018 reported that, since 2013, there have been more than 14,700 victims of tax phone scams, who lost in total at least $72.8 million to perpetrators. The Federal Trade Commission's (FTC, 2018) The Consumer Sentinel Network reported that, out of the nearly three million reports received, imposter scams ranked at the top (nearly one in five people) with a total loss of $500 million, indicating an increase in losses from the previous year. While the total number of complaints has increased during recent years in both the UK and the USA, it is unclear whether this growth is due to an upward trend in scams or an increase in reporting (ONS, 2019).

Modus Operandi and Characteristics

Although there are many types of scams (Action Fraud, 2018; Button et al., 2009), they all have similar features and follow a well-delineated pattern to succeed (Langenderfer & Shimp, 2001). Fraudsters have several ways of identifying potential victims. They may obtain victim data from open-source directories such as phonebooks or public company share registers or from 'sucker' lists, which are lists compiled of personal information of previously scammed individuals (Button et al., 2009; Levi, 2008). Gathering such personal information also takes place via phishing, an attempt to gather personal information by using deceptive phone calls, e-mails or websites proposing to be from legitimate sources (Kanjuk, 2016). All this sensitive data is stored later in large databases and used to scam individuals and taxpayers out of large sums of money (Banoff & Lipton, 2005; Levi, 2008). The information may also be sold to fraudsters in other countries (Age UK, 2015).

Scams tend to follow characteristics of organised crime, with a variation on the *modus operandi*, depending on the type of scam. Organised crime can be defined as planned and coordinated crime by individuals who regularly work together (May & Bhardwa, 2018), and fraud is typically seen as a primary activity of organised crime groups or as an enabling activity to fund other serious crimes (National Fraud Authority, 2013:10). Recent reports have linked almost half of the fraud in the UK to organised crime groups (Cifas, 2017), with the UK home office estimating organised fraud alone costs the UK an estimated £9 billion a year (2013).

Studies (Bidgoli & Grossklags, 2017; Button et al., 2009; Button, Nicholls, Kerr & Owen, 2014; Employee Benefits, 2016) have also examined the nature, execution, and characteristics of scams analogous to the phone scams covered in this study. Deception and misinformation are central to most scams, as the initial reason to contact the victim is a complete fabrication used to gain the victims attention (Brody et al, 2014). One of the ways deception and

misinformation are achieved is through perceived authority and legitimacy, two factors that have consistently been found to be a key trigger for why people fall for scams (Bidgoli & Grossklags, 2017; Button et al., 2009; Button, Nicholls, Kerr & Owen, 2014; Employee Benefits, 2016). Scammers need to gain the confidence and trust of the victim by exhibiting a legitimate, professional persona, often through the legitimate appearance of e-mails, advertisements or phone calls, legitimate sales techniques, and the names and accents of the caller (Button et al., 2009; Wood, Liu, Hanoch, Xi & Klapatch, 2018). For example, scammers may use fake IRS badge numbers and names to appear legitimate and mention the victim's name, address, and other personal information to make the call sound official (IRS, 2018). In Bidgoli and Grossklags's (2017) study of IRS phone scams, they found that most callers often had a Middle Eastern or Indian sounding accent and were mostly male.

Another common feature of a tax phone scam is the use of pressure and coercion (Button et al., 2014) to intimidate victims into going along with the scam. When impersonating a government official and claiming that a tax debt is owed, scammers will intimidate victims into paying that "debt" by threatening them with police arrest, deportation, license revocation and more (IRS, 2018) unless it is repaid immediately (Bidgoli & Grossklags, 2017; Kantor, 2020; Which, 2020). This can cause significant harm in terms of fear, shame and embarrassment to vulnerable victims, such as older and younger people (Age UK, 2015; FTC, 2018). Scammers tend to customise their scams to fit the profile of vulnerable individuals assumed to be more susceptible and financially secure (OFT, 2006).

Crime Scripts

Scam scripts are learnt and undertaken by the offenders, similar to how actors learn their roles in a play (Hutchings & Holt, 2014: p598). Crime script analysis provides a framework for

understanding the procedures of a criminal act from the point of view of the criminal (Lee, 2020), outlining the steps and actions that perpetrators go through to prepare for, undertake and complete the scam. The scripts fit the concept of schemas in cognitive science and are seen to be a special type of "event" schema that organises our knowledge about how to understand and enact everyday behavioural processes or routines in certain situations (Hutchings & Holt, 2014). In the context of a scam, our schemas lead us to over-trust someone claiming to be from a well-known and respected organisation, such as the IRS or HMRC, as that is how we are expected to behave (Laroche et al, 2019).

As noted above, scams follow a certain set of procedures and actions to be successful. In addition to this, they also tend to work from a "physical", written script laying out the successful approaches and responses to whatever situations the scammer encounters on the phone (Shover, 2003). The script is also written in such a way that it purposively confuses the victim by overcomplicating a simple transaction and, consequently, it becomes challenging for the victim to remain objective and recognise the scam (Button et al., 2009; Langenderfer & Shimp, 2001). Crime script analysis is an evolving way of understanding different types of crime, and thus can be used to foster prevention strategies (Keatley, 2018), such as limiting tax scammers from successfully luring individuals into transferring money. By conveying what steps take place for a certain offence type, the crime script analysis identifies points of intervention (Hutchinson & Holt, 2014). There are several studies into different crime types involving crime script analysis, such as sexual offending (Beauregard, Proulx, Rossmo, Leclerc & Allaire, 2007) and active shooter events (Osborne & Capellan, 2017). It has also been used to study organised crime such as online black markets (Hutchinson & Holt, 2014), drug manufacturing, and even illegal

transnational markets involving endangered species (Moreto & Clarke, 2013). The present study uses crime script analysis by applying it to tax phone scams.

Persuasive Language and the Role of Compliance in Scams

Language has been frequently used to persuade potential victims to give in to extortion or attempts of fraud. In essence persuasive language is creative and attention-drawing. Scams exploit language resources; depending on the nature of the scam or the audience the language, usually includes catchphrases, emotive words, informal expressions, metaphors and comparisons as well as factionary examples; all to appeal to the target audience or in the scam scenarios, the targeted victims (Labrador, Ramón, Alaiz-Moretón & Sanjurjo-González, 2014).

One such example is the Nigerian love letters, where the scammers attempt to persuade the victims that they need small amounts of money to gain access to some inheritance; during that engagement, the scammers build rapport and trust with the victim, to the point where often victims feel infatuated with the scammer, thus give in to any demands and become victimised. Other scenarios begin with direct love letters where the scammer pretends to be a kind-hearted person, in need of help, looking for love, to build a family and a future. Various people fall victims of such fraudulent techniques for many reasons. Some include the need for companionship, others are attracted to the idea of getting rewarded, and many allow themselves to be persuaded because of loneliness (Schaffer, 2012). That said, those scams are not as easy as they may seem. Scammers employ various techniques to achieve their goals, one of which is the utilisation of persuasive language. For example, during conversations or any other form of communication, they use flattery, appeals to greed, they apologise even if there is no need to apologise, they employ the element of altruism, trust and quite frequent speak of religious beliefs, benefits, rewards, satisfaction, and a prosperous future. In other words, they employ all

aspects that could lead the victim into believing that the person is a legitimate individual and worthy of their trust and help (Onyebadi & Park, 2012).

Such language and persuasion techniques, we see them often in advertisements and are frequently taught in sales techniques for maximising financial gain and attracting more customers (Schmidt & Kess, 1986). However, scammers also keep in mind and base their success level on the levels of compliance and conformity of the targeted individuals and potential victims. It is well established within research that people tend to conform and comply at a greater degree, when the direction, guidance, request, or direct order comes from an authority figure or an individual with some sort of power and effect (Cialdini & Goldstein, 2004). Victims do not want to comply with the scammers; in most cases victims are not aware they are being scammed and in others if they suspect the fraudulent nature of that communication, they may give in out of fear if they are threatened or any small chance of any real benefit. Some researchers see compliance with scams as a result of humans' bounded rationality or limitations on rational decision making, as well as victims' vulnerabilities (e.g., lack of education). For the latter, there are various risks factors; susceptibility to interpersonal influence is one, isolation, age, as the elderly are proven to lose twice as much due to scams, and many other factors that empower compliance with scammers' demands (Fischer, Lea & Evans, 2013).

Awareness campaigns

The HMRC and the IRS have repeatedly issued warnings of what to look out for when receiving calls in which the caller claims to be from a government department. For example, for more than 10 years, the IRS has provided the public with information on its website about, what it calls the "Dirty Dozen" list, with phone scams topping the list (IRS, 2018). The IRS gives a

detailed account of how the scam works (such as altering caller ID numbers to make it look like the IRS or another agency is calling), and states that the IRS will never use telephone calls to:

- Demand immediate payment using a specific payment method such as gift cards or wire transfer.
- Threaten immediate law enforcement action by arresting the taxpayer.
- Demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed.
- Ask for credit or debit card numbers over the phone (IRS, 2018:n.p.)

The HMRC also provides information on how to "recognise the signs of fraud" and regularly releases updates and warnings during tax filing season when tax scams tend to increase (HMRC, 2019). The same information is delivered by numerous other fraud reporting organisations such as Action Fraud (Action Fraud, n.d.), Cifas (2017) and TIGTA (2018). All these reports combined are useful for consumers and could alert taxpayers about scammers, especially during tax filing seasons (IRS, 2018). They also give some insight into the script that scammers follow when executing their scam, but there is little research reporting their scripts in detail. Knowing more about the language features and narrative content of their scripts could help expose scammers, thereby preventing victimisation.

Some features of IRS and HMRC phone scams have already been pointed out in a few published articles (see Bidgoli & Grossklags, 2017). Similar studies that relate to the present study's research objectives include a study by Schaffer (2012), which looked at detailed language features of Nigerian fraud (4-1-9) letters by examining the exact wording that was used. For example, out of the 30 letters analysed, the key words that were frequent in headings included "urgent", "business", "assistance" and "proposal," as well as appeals to legitimacy,

secrecy, and urgency in the main body of the letters. Based on the language, most of the letters appeared to be written by "minimally competent English speakers" (p.171) who were trying to use language to impress, persuade, entice, reassure, evoke sympathy, and impress the recipients on the legitimacy and urgency of the emails. Nevertheless, research is scant and tends to focus on victims rather than the scammers themselves (e.g., Bidgoli & Grossklags, 2017; Button et al., 2009; Cross, Richards & Smith, 2016; Wood et al., 2018).

The reason for the lack of research may be because scammers usually operate on an international level and are based overseas, making it more difficult for researchers or even law enforcement officers to locate scammers for interview or prosecution (Baugh, 2018). However, even if they were located, it is unknown and doubtful if they would be willing to speak to researchers or partake in any kind of research that would work against their profitable fraudulent operations. The lack of any form of motivation or beneficial reason to partake in research has made attempts to profile these criminals difficult for researchers. Regardless, some successful attempts have been made recently, on profiling such scammers (see Tzani-Pepelasi, Gavrilović Nilsson, Lester, Ioannou & Pylarinou, 2020).

Some individuals, who have managed to speak to or conduct some form of interview with scammers, particularly HMRC and IRS tax phone scammers, are Internet trolls. Trolls are usually described as "malicious practical jokers", posting unkind or offensive messages on social media sites or discussion forums with the aim of starting arguments with others (Cocking & Hoven, 2018:7; HarperCollins Publishers, 2019). Trolls have not been extensively studied, and their role is still to be defined (De Seta, 2013). However, in Internet slang, a troll is a person who sows discord by starting arguments, upsetting people or posting inflammatory, extraneous or off-

topic messages in an online community (such as a newsgroup, forum, chat room, or blog), with the intent of provoking other users into an emotional response for the amusement of the troll.

There have been a number of YouTube trolls that have managed to engage HMRC and IRS scammers in discussions and informal interviews, later uploading the video onto their YouTube channel, in an attempt to gain more insight into scamming activities and tactics, believing that the longer they manage to keep the scammers on the line, the less chance there is for another innocent individual to become victimized (Chang, 2017:n.p.). The trolls can easily gain access to the scammers contact details via online websites and blogs dedicated to providing trolls with the phone numbers of scammers, such as the website 'Ownage Pranks' (2020) who provide advice for wannabe trolls and phone numbers for numerous IRS scammers. Apart from YouTube, trolls have also used other social media channels to make people aware of scams (see Chang (2017: n.p.), such as Microsoft Tech Support Scams (Protect yourself from tech support scams, 2019). Trolls have been persistent in attempting to increase public awareness on how to recognise the fake "Mr Windows Repair Guy" (Crawley, 2019:n.p).

The Present Study

Considering the lack of relevant research on the victims of fraud and the ongoing need for consumer protection, the present study was intended to examine and describe the scripts used during the IRS/HMRC scams. This research was exploratory, and not driven by outlined hypotheses, due to the nature of the problem the study investigated lacking volume of relevant research. By conducting the present study with an exploratory approach, it allowed multiple research questions to be explored about the phenomena and provide a broader understanding on the mechanisms behind this still relatively under researched area (Stebbins, 2001). In particular, the analysis aimed to identify the steps that scammers follow in the script; the language they use

and terminology that may give away the nature of the deceitful call; the tactics they use to persuade or intimidate the victims; the amounts that the scammers aim to collect from victims; and whether they operate individually or as part of an organised crime group. However, some research questions related to this project are included in a previous publication.

Method

Data

Although this typology of scam occurs globally, the present study will be focusing on scams linked to the forementioned tax branches HMRC (UK) and the IRS (US). However, it has proven difficult to access scammers to collect data on the IRS/HMRC scams, primarily because of the detection-avoidance strategies that the scammers use. In addition, most fraudulent organisations operate overseas. Because of these difficulties, the present research utilised 30 YouTube videos to identify the scam scripts (see Table 1 for more information on scammers' characteristics). YouTube videos have been used for empirical studies in the past (e.g., Adami, 2009; Tzani-Pepelasi, et al., 2020). In the videos analysed, trolls engage with the HMRC/IRS scammers and impersonate victims either because they act as vigilantes or because they have received a fraudulent call which they record. (See De Seta [2013] and for research on Trolls).

Table 1. *Summary of Scammer Characteristics.*

Variables	n	%
Gender of scammers		
Male	27	90.0
Female	3	10.0
Accent of scammers		
No clear/native British/American English	19	63.3
Convincing to non-native English speakers	11	36.7

Asian-type English	25	83.3
Clear English (no clarity on British or American)	4	13.3
Jamaican-English	1	3.3
Language syntax and grammar		
Grammatical mistakes	14	46.7
Some grammatical mistakes	16	53.3
Threats/Intimidation		
No threats	2	10.0
Personal threats	2	10.0
Other threats	26	80.0
Surrounding Environment/Background		
Background noise resembling a call centre	27	90.0
No background noise	3	10.0
Senior officer/supervisor/ manager		
Not mentioned	9	30.0
Mentioned but not available	2	6.7
Available and involved	19	63.3
Anger management when provoked/confronted/exposed		
No anger	19	63.3
Anger	6	20.0
Ended call when confronted by troll	2	6.7
Remorse for fraudulent activity		
No remorse	22	73.3
Some remorse	6	20.0
Ended call before exposure by troll	2	6.7
Payment method		
iTunes card (IRS scam)	16	53.3
Bank transfer (HMRC scam)	3	10.0
No payment method detailed	5	16.7
MoneyGram	1	3.3
Cash withdrawal	2	6.7
Debit card details asked for	2	6.7

Stream card	1	3.3
Scammer contact with victims		
Voice mail left for call back	11	36.7
Called mobile phones	4	13.3
Called landline	1	3.3
Trolls called scammers	14	46.6
Call behaviour		
Victims put on hold/Scammers wait online for payment	28	93.3
Did not put on hold/wait online for payment	2	6.7
Communication persistence		
Would not allow call-back/Would call back themselves if call interrupted	12	40.0
Would allow call-back/called back themselves	11	36.7
Option not mentioned	1	3.3
Victims' private information		
Did not have victim's address	4	13.3
Had victim's real address	4	13.3
Gave an address that was not from victim	11	36.7
Did not mention address	11	36.7
Phishing		
Asked for personal information	27	90.0
Did not ask for personal information	3	10.0
Secrecy		
Asked to keep matter and payment method secret	10	33.3
Only referred to confidentiality of call	10	33.3
Did not mention secrecy/confidentiality	10	33.3
Exhibiting fear when exposed		
No fear	21	70.0
Some concern	6	20.0

Ended call with no sign of fear	2	6.7
Call interrupted before exposure	1	3.3
Call excuse		
Victims' owed money	27	90.0
No clear reason	1	3.3
Did not reach that point in call	2	6.7
Case reference/badge number		
Case reference but no badge number provided	6	20.0
Both provided	15	50.0
None mentioned	9	30.0
Requested amount		
Did not reach point in call to request amount	7	23.3
From $500 to 5982.32	23	26.7
File		
Pretended to pull out relevant file	24	80.0
Did not mention any file	6	20.0
Identity		
Likely fake name provided	23	76.7
No name provided	7	23.3
Scammer location		
Pakistan	2	6.7
India	2	6.7
Washington DC	1	3.3
England	1	3.3
No location mentioned	22	73.3
Use of vulgar and insulting language by scammer when confronted/exposed		
None	17	65.7
Used	12	40.0
No reaction	1	3.3
Patience by scammer		
Was patient	27	90.0
Became irritated	1	3.3
Call ended before situation requiring patience	2	6.7
Inducing fear and intimidation		

By repeating consequences of not complying/Adding new threats	27	90.0
No intimidation	1	3.3
Call ended before any intimidation	2	6.7
Verbal aggression when irritated (by troll)		
None	8	26.7
Present	20	66.7
Call ended before reaction	2	6.7

Note: Reprinted from "Tzani-Pepelasi C., Gavrilović Nilsson M., Lester D, Pylarinou R, N. & Ioannou., M. (2020). Profiling HMRC and IRS Scammers by Utilising Trolling Videos: Offender Characteristics." Copyright 2020 by *Journal of Forensic and Investigative Accounting*.

Video selection

To identify the appropriate YouTube videos a search was performed using the following key words: 'IRS tax scamming', 'HMRC tax scamming', 'trolling tax scammers', 'tax scamming', 'phone tax scamming'. The search resulted in several videos which contained trolls engaging in a phone conversation with HMRC/IRS scammers who believed that the trolls were genuine targets. The dates of the videos that were selected ranged from 2016 up to December 2018. 68 videos were selected initially but after a thorough examination of the videos resulting from the search, only 30 videos were selected using the following criteria:

- Videos were longer than three minutes.
- The troll entered a discussion with the scammer and the scamming technique was revealed.
- The trolls were individuals that aimed to keep the scammer on call for as long as possible without engaging in unnecessary foul language.
- The videos were in English.
- The content of the videos was solely related to the IRS/HMRC scams.

The inclusion of the videos was limited because the videos needed to have sufficient communication time for the scammers to reveal the full script, or at least most of the scam prior to realising that he/she was being trolled. It should also be mentioned that the trolls aimed to keep the scammers engaged as much as possible under the impression that if the scammers are preoccupied, a victim is saved from being scammed. It should also be mentioned that the videos were watched by two researchers at the same time and there was full agreement on which ones were potentially useful for analysis and which were excluded.

Speaker Profiling

Speaker profiling is used as a forensic investigative tool when there is an unknown offender and when investigators need to narrow down the suspect pool by identifying linguistic features and speech patterns that can be linked with geographical areas, social groups, or pathologies, for example, smoker's voice (Schilling & Marsters, 2015; Watt, 2010). Experts, such as speech analysts, can use a variety of methods, such as aural-perceptual, acoustic phonetic and automated analysis to carefully examine voice quality, rhythm and speech patterns using quantitative, objective, and replicable methods, which are often accepted by courts as valid expertise evidence (Watt, 2010). However, speaker profiling can also be performed by non-experts or listeners who can use simple auditory analysis, that is, listening to build a profile, relying on previous experience of voice and language varieties (Watt, 2010).

In the present study, speaker profiling was used to ascertain a scammer's characteristics such as gender, accent, and language use, including sentence structure and verb tense, to gain insight into the individuals who might be engaging in IRS/HMRS scam calls. Other characteristics identified were related to the techniques used to persuade potential victims that the call is legitimate and, thus, get the victims to comply with monetary demands. Two members

of the research team watched the videos at the same time and examined the aforementioned aspects. There was full agreement on the aspects that were included in the analysis (e.g., gender, non-English accent, vocabulary), prior to conducting the content analysis.

Results

IRS/HMRC Scam Script and Steps

The present study used the 30 videos to analyse the content and reveal the pattern of the scam. All 30 videos were used for qualitative and content analysis. Parts of some of the cases are presented below for a deeper understanding of the script. Many of the quotes result from three different videos and were purposively selected as the scammers in those videos did not deviate from the sequence of the scripts, while also did not jump any steps. Although it should be mentioned that from the analysis of the 30 cases, it appears that these types of scammers follow a script from which they deviate according to each scammer's techniques, skills, experience, and level of English spoken. It is highly likely that they are part of organised crime groups. They may be part of the same group or different groups. Based on the scammers' behaviour, it is assumed that they are part of different groups. An indication of this conclusion is the difference on the way the scammers would maintain the order of the steps or jump steps and return later, during the conversation. However, this is only an assumption and cannot be confirmed. It is also highly likely that the scammers acted differently because of the level of experience. It could be assumed that a more experienced scammer used the steps as he/she show fit and appropriate for that victim. Whereas a less experienced scammer would have to stick to the provided script. The script and process steps are detailed below, and parts from the transcribed conversations are presented as examples. The conversations presented below are as transcribed, including the grammatical errors. The steps are summarised in Figure 1 below.

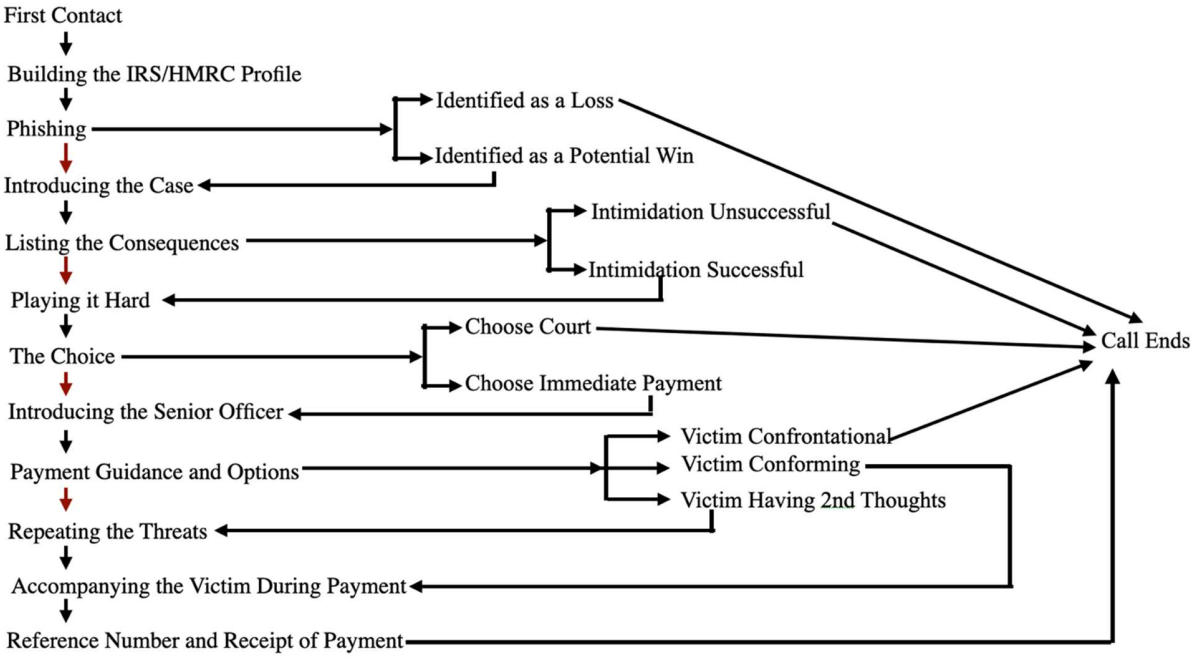

Figure 1. *Representational Summary of the Scam Script Steps.*

From the 12 established steps in the process of this scam, four overarching themes were developed, highlighting a potential framework the scammers use when carrying out this particular scam typology. The themes are based on the common steps used by the scammers. It should be mentioned that this project is off exploratory nature, therefore the themes were created based on the agreement of the involved researchers. The resulted themes are representative of the included content and indicate the intentions and purpose of the steps the scammers utilised to achieve payment. The results are presented as a narrative of findings, in the chronological order they appear in the proposed framework of the scam.

Building Credibility

First contact with the victim: This occurs either by leaving an emergency voice mail or by a direct call informing the victim that the IRS/HMRC will be taking legal action against the victim (53.3% of sample)

Troll: Which company is this?
Scammer: This is the IRS; Scammer: Internal Revenue Service how can I help you?
Troll: Hi, yeah, I'm just returning your call

Many of the trolls find the fake IRS/HMRC numbers and call to prank the scammers (43.6% of sample), pretending that they are legitimate victims who are responding to the call or voice mail left by the scammer (Chang, 2017; Crawley 2019).

Building the IRS/HMRC profile: Introducing themselves as IRS or HMRC officers.

Scammer: Who are looking for?
Troll: My name is Cristopher Molo
Scammer: Okay. You know what time is received a phone call from us...?
Troll: Yeah just a few minutes ago actually
Scammer: So how can I help you Philip?
Troll: I, uh, you called me. You said that, uh, it was an urgent call from the IRS
Scammer: This is the IRS.
Troll: I am a bit nervous as I have never been in trouble before.
Scammer: Write down the warrant number please.

The IRS and HMRC frequently issue warnings about how to recognise scammers who often use fake names and badge numbers to identify themselves to appear legitimate (IRS, 2019). It is common for the scammer to willingly provide their fake badge number and a case reference number (50% of sample). By doing so, many potential victims might be under impression that a legitimate governmental employee or representative has contacted them.

Phishing: Asking the victim for information about their previous tax records and attempting to find out whether the victim is a potential win (90% of sample). This often occurs if the victim mentions that he/she does not remember their tax filling records of previous years.

Scammer: ok. I would like to ask you one more question. Have you ever faced any kind of criminal cases?

Troll: No. No. Goodness me. I've never been in any kind of ...I mean I got a speeding ticket once, but I paid that off immediately.

Scammer: So, have you ever get arrested?

Troll: No.

Scammer: For any purpose, like any custody, have you ever went into custody for any purpose?

Troll: No. Goodness me no.

Scammer: No? Listen. I want you to be very honest because you are in a recorded line and now, I am going to check your records, your past records, if we found any records, any bad records, then you won't get any chance. Strictly. We will forward the police department; I mean we will forward these papers to your police department and let this case handled by your local police department.

In this example poor wording it is evident. The scammer has put the troll in the position of confessor, asking if there is a criminal record that would make things harder, whilst phishing for information that could be utilised to persuade the victim to pay the allegedly owed amount. If the scammers play the odds and, if a victim does have a criminal record, it will enable the scammer to instil more fear into the victim which increases the likelihood of the victim complying with paying the required sum instead of risking imprisonment. Moreover, the scammer reminds the troll of the recorded line to keep up his appearance of legitimacy, while informing the victim that he has the power to check the troll's criminal records.

Troll: No. I've never been… mean it was the speeding ticket but that was 10 years ago that I got that speeding ticket.

Scammer: 10 years ago?

Troll: Yea. All I got was a fine for that. I have no criminal record.

Scammer: I am just checking your records. (on hold for 10 seconds). Mr. Smith hold the call, I am just going to speak to my supervisor.

The latter implies that by speaking to an alleged supervisor, the scam and the process could appear legitimate. Another reason could be that the scammer is being cautious or has become suspicious because the troll was perhaps too conforming and calm. It is highly likely that, when victims are informed of such accusations, they become emotional and perhaps lose their temper. Moreover, during such conversations the scammers use "we", indicating that he/she

is not working alone and that this team is sharing knowledge of the actions and replies, as commonly occurs in organised crime (May & Bhardwa, 2018).

Introducing the case: Informing the victim of the alleged tax offense and why the IRS/HMRC is taking legal action against them, for example, that there are miscalculations in their previous tax reports (90% of sample).

Scammer: It's my job to inform you, before I proceed ahead, that this line is recorded and monitored by the HMRC headcounter as well as the judicial courthouse. Even your local state authority is the attorney's general office, and I will appreciate it if you don't interrupt me when I speak and listen to me very carefully, I promise I will give you fair amount of time to raise your questions. Ok?

Troll: Ok

Scammer: Ok. Here is what happened. The HRMC have conducted a pre-audit on your tax filing for the period 2010-2016. I am talking for the last 6 years. And when we completed that we found that, under section 1 50 of the ITA income tax, that you have inappropriately underpaid your taxes. And the amount of £3994 has underpaid by you. Now, it is claimed that it was underpaid or it was kind of miscalculations).

The scammer's attempt to persuade the "victim" of the call's legitimate nature begins immediately as he adopts an authoritative tone of voice and instructs the troll to carefully listen to the "facts". From the first, he informs that the line is being recorded. However, most legitimate call centres have automatic systems stating that the line is recoded for training purposes when a customer calls. In addition, most governmental organizations have an automatic system that leads the customer to the correct call centre and employee by choosing, among various options for the most relevant purpose of the call (e.g., press 1 to….., press 2 to…..etc.).

Fear Mongering

Listing the consequences: Telling the victim what all the possible outcomes of the legal action may be. The scammer has informed the victim of the reason for the call in the previous step. Next the scammer emphasises further the allegedly made mistakes.

Scammer: When you filling your taxes, you must be very correct with the digits because even one digit can lead to miscalculations. And in this case it is called a miscalculation error.

And in your case in duration of all these years there was several errors in your taxes. And we strong evidence to believe, well we have reason to believe that it was negligence, but also an act to defraud the HMRC. Because we tried to notified you with letters twice in your house. But you were not home. We need your signature to deliver those letters. We are not authorized for that. We are not responsible for that.

The scammer declares that the victim has a period of six tax-filing years during which taxes have been underpaid. This may easily confuse the taxpayer as it can become difficult to remember tax-filing details from a few years ago. In addition, fake article sections are mentioned to further persuade the victim of the call's legitimacy and the seriousness of the situation. The scammer is fishing as he informs the victim that he had perhaps mistakenly underpaid because of a miscalculation. In this case, if the victim had indeed happened to have filled miscalculated tax reports in the past and had become aware of that, then he would have been persuaded that the call was legitimate. It can be apparent that there are many structural mistakes and a lack of appropriate wording, indicating the scammer's poor level of English (47.7% of sample). The scammer also informs the victim that the HMRC did the best they could to notify the victim of the situation and mailed a letter to his house. However, nowhere in the discussion has the troll given an address, nor asked the victim to verity his address.

Scammer: You were not responding for the yellow slips we left to your house. HMRC thought that you were trying to run from the HMRC. You were trying to hide. In this case, this is the only reason there is a serious legal case against you has been filled to the courthouse regarding for a serious allegation on name. These serious allegations are: count number 1 violation of revenue tax revelation. Count number 2 violation of HMRC taxation code. Count number 3 theft by deception. Count number 4 wrongful misrepresentation, of information are tax evasion and tax avoidance to the government organization. So at this point of time we have decoded to forcefully recollect this amount from you by involving the HMRC court PSLA2011-18 against you.

To make this call appear to be an HMRC legitimate call, the scammer mentions the "yellow slips" that the HMRC representative left at the victim's house as a last attempt of notification. The scammer accuses the troll of trying to hide from the HMRC and begins

counting “allegations”. From this section, it becomes even clearer that the scammer’s English language usage is poor. It seems that these statements are made to appear formal, but also to confuse and scare the victim (90% of sample). The various named article sections and the structure of the whole statement implies a script that these scammers follow.

Scammer: What this court means to you is HMRC will (word not understood) on your personal assets. And that means even including your house, car, and all your know bank account will be frozen started today. I can also be published in local media and local newspapers with reason of adding to the proof. Any existing payments plan with the HMRC will be terminated under section 38F HMRC code. In addition to recoding criminal conviction the courthouse may impose security bonds, community service, additional penalties and for some often imprisonment sentence. Passport, state and your driving license will be ceased and they will also file a (word not understood) deception under section 11A. Now if you have any questions please go ahead and ask me before I sign up you case papers and forwarded to the higher authorities.

Playing it hard: Informing the victim that there is nothing that they can currently do to stop the legal action being taken against the victim. This amplified effect of fear by the stated consequences may cause HMRC customers to overlook the fact that UK taxpayers do not file their taxes like taxpayers in the United States. If the legitimacy of the scammer is strongly assumed, then the victim may begin to doubt themselves and their previous tax activities. In the previous part, the scammer begins the intimidation technique by informing the troll of the serious consequences, including imprisonment. To further strengthen the effect of the alleged consequences, the scammer asks the troll whether he has any questions before he forwards the documents to the higher authorities. The scam call is threatening and pressures victims into acting quickly. This is a common sign of a scam as it is designed to stop victims from thinking through their actions (Bidgoli & Grossklags, 2017; Kantor, 2020; Which?, 2020). The scammer attempts to manipulate the troll into requesting for help and alternative solutions to the problem. This will ultimately lead to the next step of the scam - giving the victim/troll a last chance to make things right by paying the owed sum right away.

Troll: I have never been in any trouble before. I don't want anything against me. So what do I need to do?

Scammer: Fist question I want to ask you is why you didn't response for the yellow slip?

Troll: Well, I live, I rent the lower apartment of a large house from an elderly couple so sometimes I don't receive my mail. So it might have been that the slip was left upstairs and never came to my post downstairs. That is the only thing I can think of. I never saw the slip. –

Scammer: You never get a slip?

Troll: No.

Scammer: Are you serious that you never receive a slip?

Troll: Yes, yes, absolutely. I wouldn't lie.

The scammer asks this question to maintain the character of an IRS/HMRC official that he is impersonating. However, when the troll informs the scammer that he never received a slip the scammer responds by asking, "Are you serious?". An IRS/HMRC employee would not respond in this way, and this is not part of IRS/HMRC training materials. It is assumed that the scammers are trained to enrich the script that they are given and, by doing so, they expose themselves. It is signs like these that the IRS/HMRC and other consumer consulting websites and even internet trolls warn the public about in order to equip individuals with the knowledge that they need to recognise any scam calls they may receive (Action Fraud, n.d.; Chang, 2017; HMRC, 2019;2020a).

It is assumed that, if the scammers are allowed to enrich the scamming script, they will add their own way of expressing information.

Scammer: Because the officer that was an HMRC officer of the local department came physically at your doorstep to deliver this documentation. But as you was not present at your home, the officer he drop a yellow slip at your doorstep and that slip was to notify you to collect your document at your local post office. And for three days the documentation was lying down inside yellow code post office and after three days the documentation was bounce back to us and since that you are trying to fraud with the government with an intention.

Troll: Well no, no. Obviously I would never do such a thing. I didn't know that anyone had come physically at my doorstep at all).

In this case, it is obvious that the poor choice of wording, sentence structure mistakes and the wrong article choices can expose the scammer (Bidgoli & Grossklags, 2017; Schaffer, 2012).

In the last question, the scammer repeats the previous statement, while adding new information, this time involving the post office, another governmental organisation, to enhance the perceived legitimacy of the call.

Providing Hope

The choice: Informing the victim that there might be a solution if the victim pays the whole amount owed at once.

Scammer: Hello Mr Smith, I have just check your records and you have good records. Ok. As I talk to my supervisors as well as with my senior officer, this gives you an option. You will be having two options right now. You have to choose an option and you need to give an answer. Right now either you need to have a good solicitor for yourself who will be able to challenge the government and will be able to represent you inside the court. I mean you need to fight this case or you need to resolve this by today sir in immediate pace. I will explain all that. If you chose to fight this case, you need a good solicitor who will represent you inside the court and if you win this case you will not have to pay a single pound and nothing. But in case if you lose this case the charges might be up to £20,000 to £25,000.

Troll: Oh gosh.

Scammer: And if you lose this case, according to section 101, each and every whatever you have under your name will be ceased by the federal government.

The scammer supposedly checks the victim's criminal records (93.3% of sample), and the records come clean or as he says, "good records". Moreover, this time he involves a third person whom he names as the senior officer (63.3% of sample), and he implies that, for the case to be dealt with, his supervisor and the senior officer, as well as himself, must become involved. The scammer continues with the next step, that is, to inform the victim of his or her current choices. The first choice is to hire a "good" solicitor to fight the case in court, but the scammer intimidates the troll with the possibility of losing the case and having to pay six times the initial amount.

Scammer: And another option to you is that, if you are willing to resolve outside of the courthouse before we take this case inside the court, what you need to do is you need to make a quick payment to the government in with a paysis in order to cancel all the charges in you name which you have.

Troll: Right.

Scammer: So my question to you is what you are willing to do so I can update this to my senior officer and also have a word with my senior officer.
Troll: Well I certainly prefer to resolve this today if that is possible. I would rather, I mean I have never had to deal with a solicitor before and would rather not.
Scammer: Ok. So you mean you want to resolve this with a paysis. Correct?
Troll: Yea.

Introducing the senior officer: If the victims agree to pay, they are told that only the senior officer can accept any payment, and they are subsequently connected to a "senior officer".

Scammer: Ok. In this case what I am going to do is I am going to connect this line to my senior officer who is authorized person to give you all the information and to resolve this case.

The new option for the troll is to resolve the matter without involving the court, and this can be achieved by paying the amount immediately. This seems to be a common feature of IRS/HMRC scams. Typically, the calls sound urgent, pressuring the victim to take action to avoid legal and financial consequences (Bidgoli & Grossklags, 2017; Kantor, 2020). The scammer claims that this option can only occur if it is organised by a senior officer and, therefore, transfers the call again. This, again, is an attempt to make the call seem more legitimate (Wood et al., 2018).

Scammer: Ok? Now you talk to my senior officer.
Troll: Ok. Thank you.
Scammer: You are welcome, and I really appreciate your time and patience.
Troll: Ok. Yes. Thank you, sir.
Scammer: (Another scammer is on the phone). Thank you for holding. This is the senior investigating officer. My name is Robert Peel. Can I help you?
Troll: Hi. I was just speaking to your colleague and he just said that I can possibly resolve this matter today.
Scammer: Oh. Can I ask to whom I am talking to?
Troll: Yes. My name is John Smith.
Scammer: Your name is John Smith?
Troll: Yes.
Scammer: Hallo John. How are you doing?
Troll: Ok, I guess. I am a bit worried about this matter. I've never been in any kind of trouble before.

A different scammer is on the line now, the accent is slightly better, and gives a fake Western name (76.6% of sample). The use of fake anglicised/Western names is a common feature of scam phone calls and is an attempt to increase the authenticity of the calls (Ministry of Justice, 2017). This scammer asks for the troll's name. This can be either to test the troll to see if he is telling the truth and reports the same name as initially, or because he does not know who this person is. If this is the case, then the scamming team appears to be disorganized.

Payment guidance and options: Explaining to the victim how they should transfer the payment to clear their debt and avoid legal action. In most IRS cases, victims are told to pay using iTunes cards (53.3% of sample), while for HMRC there are cases where a direct bank transfer or Western Union transfer has been requested (16.6% of sample). During the call with the senior officer, there is a further attempt for intimidation.

Scammer: (hums). Ok. John the thing is that, right now, there is nothing, there is no option to pay this back. Right now, we are about to proceed this case legally. In 20 minutes, I would have to sign the papers up and take it to the court.

Troll: I thought your colleague said that I could resolve this today?

Scammer: I am not sure whether I can do it or not. I would have to speak to my senior officers to see if there is any possible that you can resolve this.

Troll: I thought you were the senior officer.

Scammer: Yea. I am senior officer but I would have to talk to my senior officers.

Troll: Right. Ok. I want to resolve this, if possible, today. I don't want it to go on my record. It might affect my job.

Scammer: Ok. To inform my senior officers, do you have enough to cover the full amount?

Troll: Can you remind what the full amount is?

Scammer: It's £3.994.

In this part, the scammer appears persuaded that the troll is a legitimate potential victim and revokes the second option that the first scammer gave during the first discussion. This may be because of the disorganization of the team as mentioned earlier or because it is a tactic to further scare the potential victim. In this conversation the "senior officer" informs the victim that he would have to talk to his senior officers to allow the second option as a solution (63.3% of

sample). This indicates that there may be ranks in the fraudulent organisation. It may be that victims do speak with more than one or two individuals during the progression of the scam, and this may very well be to cause confusion or because some scammers are more skilled than others and get the job done faster. This scammer asks the troll if he has the full amount available in order to resolve the matter, and the scammer mentions the full amount as initially stated. It can be assumed that either scammers have a common script, and all victims are requested to pay the same amount or that the first scammer had notes that he passed on to the second scammer for reliability and consistency.

Dissolving Doubts/Securing Payment

Repeating the threats: If the scammer notices that the victim is delaying or having second thoughts, the scammer will repeat the legal consequences of their actions and add new ones that might be more personal and frightening to the victim according to the information the scammer has managed to gather from the victim about the victim's personal life and circumstances (90% of sample).

Troll: Is there any other way to fix it?
*Scammer: You're supposed to be at your place. The documentation the *inaudible* subpoena will be received by you and you will be under custody for next 72 hours and then you will be presented into the courthouse. You can prove this inside the courthouse okay.*
Troll: Why – so why – I'm gonna be arrested?
Scammer: Yeah, within – as this line will be disconnected within 45 minutes or an hour you will be arrested okay).

This particular step can also take place during the payment process if the victim shows signs of having second thoughts.

Accompanying the victim: The scammer insists on staying on the line until the victim has bought the cards (for IRS) and given the numbers over the phone for the amount to clear (93.3% of sample). This can take one or more hours if the victim has to drive to a store to

purchase the cards. In HMRC cases, the scammers go through more details about the victim's assets and funds.

Troll: Yea. I have to take it from savings account but yea I've got that.
Scammer: You'd have to get it out of your savings account but you have it?
Troll: Yea.
Scammer: Let me see what I can do sir. Can you give me your debit card number?
Troll: Yea, hold on. And if I give you my debit card number this will be resolved today? It won't go any further?
Scammer: Right.
Troll: Right. Ok. It's ….well the money is not on my debit card though.
Scammer: Sir I would have to update that he is providing the details and then they will go further).

In the last part of the conversation the scammer asks for the troll's debit card number; and this is a major difference between the IRS and HMRC scams. In most IRS scams the scammers ask for iTunes cards, which they call "federal approved payment", but the HMRC scammers ask for debit cards (see Tzani-Pepelasi et al., 2020). This could be because iTunes cards are commonly used in the USA but, in the UK, are not preferred. Instead, in the UK, paying with a debit card over the phone is very common and normal. Following the latter part of a discussion, the troll confronts the scammer, which results in vulgar language use and threats. Bidgoli & Grossklags (2017) also found that scammers tended to get particularly aggressive when the victims did not follow their requests (66.7% of sample).

Another example shows the scammer further intimidating the victim with arrest threats if the victim disconnects from the line.

Scammer: So first of all. Let me tell you the most important thing. We are working over federally monitored and recorded phone line and all this phone line are attached to computer system management. The minute this call get disconnected the warrant is going to execute. So we have to stay on line unless and until we cancel the warrant. So…are you speaking through your cell phone or your home phone, sir?

Likewise, a similar example (IRS) shows the request from the scammer to stay on the line with the victim till the payment is complete.

Scammer: Today first of all withdraw the cash from the bank. Once we get the cash just let me know I'm on the line, you need to stay on the line with me itself, okay?

Troll: Alright alright. So, I just leave the line – just leave the line open then? I'm gonna leave now, I'm getting my shoes on. I'm just gonna drive down to the bank it's only right down the street.

Scammer: Okay, no problem.

Troll: Alright, alright, alright. Uh, when I get to the bank where do I have to go next?

Scammer: I'll give you the address.

Troll: I'm almost to the bank right now – I'm pulling into the bank in two minutes.

Scammer: Okay, no problem. Once you reach the bank just let me know.

Troll: Yeah I'm just about to pull into the bank. I'm just waiting for the light to turn green. I'm just getting to the bank right now. I'm just about to..I just pulled into the bank. I'm about to go inside, uh, you want me to leave the phone in the car?

Scammer 2: You at – you at Walmart? You at Walmart right now?

Troll: You told me to go the bank! I have – I have to get the money!

Scammer …Yes…you're right. So you're near your bank right now?

Troll: I am at it. I'm about to go inside.

Scammer: Okay so just – just take out $20,000 dollars and just call me back, okay?

Troll: $20,000 dollars?...He – he just told me…? - call ends.

It is evident from this part of a conversation that these scamming organisations operate both in the UK and the USA. Evidently, the scammer gets confused and speaks to the potential victim for Walmart when initially had instructed him to go to the bank. This could be because of lack of training or not paying attention. It could also be assumed that these fraudulent organisations provide the same script for both IRS and HMRC scams, leaving the scammer to amend the script as the case progresses. Moreover, a common step found in the examined videos showed that victims were instructed to maintain secrecy throughout this process, although this instruction can occur at any time of the call (33.3% of sample)

Reference number and receipt of payment: Informing the victim that the store receipt of the iTunes cards (or the transaction number if the payment is via a debit card) is the payment reference number, which the victim must hold onto as proof of payment.

Scammer: When you do the MoneyGram to the officer. The store people will provide you a receipt. They will give you a receipt. And that receipt, there will be a reference ID number, okay?

Troll: Alright.

Scammer: This I'd number, you will have to give it to me right away so that I can send to the investigating officer in order to cancel and stop the warrant. So…let me tell you, sir, in order to do this, if you are choosing to make any payment, we are not authorised to take payment from your credit card, your debit card or your bank details).

Discussion

It has been established by past research (Age UK, 2015) that scammers will continue to develop new ways of identifying potential victims and profiting on victims' gullibility and lack of awareness (HMRC, 2019). The IRS/HMRC tax scams are not new, but are under-researched, mainly due to the fact that such organised crime industries operate in countries where the western authorities have no jurisdiction. In the meantime, the losses reach millions every year (FTC, 2018; UK Finance, 2019), leaving the victims ashamed, financially damaged, and frequently with mental health issues that can even lead to suicidal behaviour (Gorden & Buchanan, 2013).

These fraudulent organizations operate on the basis that they can persuade victims that they are legitimate governmental officials. To achieve their goal, the employees of such operations are provided with a script (Shover, 2003) after their training period, and are deployed to scam as many victims as possible per day, particularly during the tax filling periods. As mentioned previously, research on this scam is limited and still developing, while restricted by the difficulty of infiltrating such operations to gather information (Tzani-Pepelasi et al., 2020). However, considering the severity of the consequences and the need for public awareness (IRS, 2018), this project analysed YouTube videos of legitimate taxpayers and trolls that engaged with IRS/HMRC scammers to waste the scammers' time and prevent them from victimising gullible victims. The aim of this project was to analyse the conversations between the trolls and the scammers to identify the script steps and the process from start to end of the scam.

The Script and the Steps to a Successful Scam

The analysis highlighted a potential framework that scammers adopt and showed that the scammers initiate the first contact either by a direct phone call or by leaving an urgent voice mail. Such information often uses databases that the fraudulent organizations have accumulated over time, or from the suckers list, and even by infiltrating the IRS and HMRC (Hadnagy, Fincher & Dreeke, 2015). If the victim is unaware of such scams, then he or she is highly likely to respond to the call. If that occurs, then the scammer identifies the individual as a potential win, which leads to the initiation of the script. The script usually begins with phishing for information and introducing the case. In many cases, the scammer even provides a fraudulent badge number to convince the victim. Next, scammers list the consequences, which in many cases are unrealistic, such as property loss and imprisonment and even removing minors from the victim's care. The intimidation technique can result in the termination of the call if the victim is aware of the IRS/HMRC processes. But if the victim is unaware, there is increased risk of successful intimidation, which leads to the next step of the script. In this step, the scammer confuses the victim by stating that there is no payment option unless a senior authority person approves such a transaction, which ultimately leads many gullible victims to plead for help. Up to this step, usually the scammer may raise suspicions due to the language barrier and grammatical mistakes, as well as unprofessional behaviour.

However, if the call is passed to another scammer identified as a senior manager, the persuasion techniques become stronger, and the second individual appears to be more experienced and with better English language skills. It is here that the victim is given the choice of paying the allegedly owed amount or proceed to a court dispute. However, scammers, to ensure payment, can alter the script and state the consequences once more. If the victim is persuaded, scammers proceed to provide the means of payment, which must be completed in

secrecy from other family members or any other members of the public. Victims are also told that, if they end the call or if the call gets disrupted, then the police will issue a warrant that will result in the victim's arrest. In many cases, the scammers ask the victims to remain on the line even while driving to the bank or to a shopping mall to make the payment over the phone. Should the victims follow all the steps, and the scammer succeeds in receiving payment, they are told that their payment reference number is either the transfer transaction number or the number of the iTunes card (only for USA).

Prior to this research, little was known about the way scammers operate. The only available information would come from police data, gathered from victims. This project gives the opportunity to the authorities to understand the way those scammers operate through a direct source. It also increases awareness and provides the steps to the public thus assists taxpayers to protect themselves from fraudulent individuals and operations. Moreover, as stated earlier, this project could be considered as a steppingstone for future research. As explained previously, direct communication with scammers and fraudsters is next to impossible. By utilising cautiously, the material and the videos that trolls publish online, researchers can build upon this research further and assist in the ultimate target, which is understanding the techniques, inform and protect the public.

Limitations and Future Research

The nature of this study was exploratory, therefore leading to some limitations related to reliability and validity. It must be mentioned that the included videos are not heavily edited, while the trolls would usually initiate the video with a description of what they were about to do, followed by the call process. Those videos were first live for the YouTube channels' users and thereafter uploaded by the trolls are permanently stored videos in those channels. Still, the researchers had

no control over what information could or would be gathered by the trolls and had no access or communication with the trolls. Consequently, it is possible that some information that could have been used for this project were omitted during the editing process. Nonetheless, due to the limited related literature, the project functions as a steppingstone for future similar project. While similar issues can be faced with traditional methodologies and data gathering processes, such as surveys where the researcher cannot be certain that all provided information by participants is legitimate. Future research could attempt collaboration with such trolls for a more controlled project. Another limitation is related to the generasability of the results. As the project focuses on IRS and HMRC scams, results cannot be generalised to other countries. However, it is assumed that similar scams take place in other countries where the organised crime industry employs similar scrips. Regardless, this can only be addressed with a future project that will explore other western countries in relation to tax scams.

In addition, the data originates from only 30 YouTube videos, which poses another limitation in terms of the sample size. However, as mentioned in the literature, approaching, and infiltrating such operations is next to impossible. It should be mentioned that there is an enormous amount of trolling YouTube videos. However, many of these videos were deemed were inadequate for research purposes, as trolls would reveal their deceitful nature from early on during the call, or they would engage in confrontational disagreements, resulting in unfinished scripts. Future research could replicate the study with more videos, as new material is uploaded on YouTube frequently. Future research should also investigate exploring the highlighted framework further, as it may provide further knowledge on the generalised structure of the scripts used in this typology of scam.

Conclusion

In-spite of the limitations, the findings can be used to increase public awareness, assist potential victims to recognise fraudulent calls, prevent victimisation and alert the public particularly during the tax filling periods. Awareness campaigns can utilise the steps that are identified in this project and inform the public, thus decreasing the chances of a taxpayer becoming victimised. Moreover, the project can be of use to authorities, which aim to combat fraudulent activity and protect the public from victimisation, for example, the authorities can utilise this project but also the sources of the data and similar sources, to pinpoint locations of the fraudulent organisations, as well as deleting the numbers from which those calls are made. Moreover, by making the public more aware of the hallmarks of these scam typologies, they are not only less likely to fall victim to these acts of fraud but can also boost awareness of the specific scam to other potential victims and law enforcement, by reporting the number the scammer contacted them on. This will not only increase the efficacy of law enforcement efforts to prevent and track these scams but potentially reduce the impact on financial debt that these scam operations have on governmental bodies.

References

Adami, E. (2009) 'We/YouTube': Exploring sign-making in video-interaction'. Visual Communication, 8 (4): 379– 400.

Action Fraud. Government agency scams. Retrieved 8 May 2019, from https://www.actionfraud.police.uk/a-z-of-fraud/government-agency-scams.

Age UK. (2015). *Only the tip of the iceberg: Fraud against older people—Evidence review*. London. Retrieved from https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and- briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf

Baugh, C. (2018, September 21). Organized crime in Mumbai responsible for popular CRA phone scam. *iPhone In Canada*. Retrieved from https://www.iphoneincanada.ca/news/cra-phone-scam/.

Banoff, S. I., and Lipton, R. M. (2005). Dirty dozen, part iv: This year's scams IRS does not want taxpayers to fall for. *Journal of Taxation, 102(5)*, 319.

Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B., & Allaire, J. F. (2007). Script analysis of the hunting process of serial sex offenders. *Criminal justice and behavior*, *34*(8), 1069-1084.

Brody, R. G., Haynes, C. M., & Mejia, H. (2014). Income Tax Return Scams and Identity Theft. *Accounting and Finance Research, 3*(1), 90-95. https://doi.org/10.5430/afr.v3n1p90.

Button, M., Lewis, C., & Tapley, J. (2009). *A better deal for fraud victims: Research into victims' needs and experiences*. London: National Fraud Authority. Retrieved from https://researchportal.port.ac.uk/portal/files/1924328/NFA_Report_1_15.12.09.pdf.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Journal of Criminology, 47*(3), 391-408. https://doi.org/10.1177/0004865814521224.

Chang, A. (2017). I trolled my IRS scammers for weeks. I learned something really dark. Retrieved 14 May 2019, from https://www.vox.com/first-person/2016/10/18/13276464/irs-scam-phone-cartoon.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology, 55*(1), 591-621. https://doi.org/10.1146/annurev.psych.55.090902.142015.

Cocking, D., & Hoven, J. (2018). *Evil online*. Hoboken, NJ: John Wiley & Sons, Inc.

Crawley, C. (2019). Don't Taunt Fake Microsoft Tech Support Scammers, Just Hang Up!. Retrieved 28 September 2019, from https://www.makeuseof.com/tag/just-hang-shouldnt-taunt-fake-tech-support-scammers/.

Cross, C., Richards, K., & Smith, R. (2016). The reporting experiences and support needs of victims of online fraud. Retrieved 14 May 2019, from https://aic.gov.au/publications/tandi/tandi518.

De Seta G. (2013). FCJ-167 Spraying, fishing, looking for trouble: The Chinese Internet and a critical perspective on the concept of trolling. Retrieved from http://twentytwo.fibreculturejournal.org/wp-content/pdfs/FCJ-167Gabriele%20de%20Seta.pdf.

Federal Trade Commission. (2014). Government Imposter Scams. Retrieved from https://www.consumer.ftc.gov/articles/0048-government-imposter-scams.

Federal Trade Commission. (2018). *Consumer Sentinel Network Databook 2017*. Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book- 2017/consumer_sentinel_data_book_2017.pdf.

Federal Trade Commission. Consumer Sentinel Network. Retrieved from https://www.ftc.gov/enforcement/consumer-sentinel-network.

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? the psychological determinants of scam compliance: The psychology of scams. *Journal of Applied Social Psychology, 43*(10), 2060-2072. https://doi.org/10.1111/jasp.12158.

Gorden, C., and Buchanan, J. (2013). A systematic literature review of doorstep crime: Are the Crime-Prevention strategies more harmful than the crime? *The Howard Journal of Criminal Justice, 52(5)*, 498–515. doi:10.1111/hojo.12036.

Hadnagy, C., Fincher, M., and Dreeke, R. (2015). *Phishing dark waters: the offensive and defensive sides of malicious e-mails*. Wiley.

HarperCollins Publishers. (2019). Troll. *Collins Dictionary*. Retrieved from https://www.collinsdictionary.com/dictionary/english/troll.

HM Revenue & Customs. (2019). *HMRC warns of landline scams threatening households*. Retrieved from https://www.gov.uk/government/news/hmrc-warns-of-landline-scams-threatening-households.

HM Revenue & Customs. (2020a). Examples of HMRC related phishing emails and bogus contact. Retrieved 16 August 2020, fromhttps://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-and-customs-examples.

HM Revenue & Customs. (2020b). *Self Assessment customers warned about scammers posing as HMRC* . https://www.gov.uk/government/news/self-assessment-customers-warned-about-scammers-posing-as-hmrc.

Home Office. (2013). *Understanding organised crime: estimating the scale and the social and economic costs* (73). Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246390/horr73.pdf.

Hutchings & Holt, (2014). Social Research about Online Crime: Global Range of Topics and a Systematic Analysis of Research in Lithuania. Accessed at https://www.zurnalai.vu.lt/kriminologijos-studijos/article/view/24959.

Internal Revenue Service. (2018). *Phone scams pose serious threat; Remain on IRS 'Dirty Dozen' list of tax scams*. Retrieved from https://www.irs.gov/newsroom/phone-scams-pose-serious-threat-remain-on-irs-dirty-dozen-list-of-tax-scams.

Internal Revenue Service. (2019). IRS warns of new phone scam using Taxpayer Advocate Service numbers | Internal Revenue Service. Retrieved 16 August 2020, from https://www.irs.gov/newsroom/irs-warns-of-new-phone-scam-using-taxpayer-advocate-service-numbers.

Internal Revenue Services. (2019). *IRS: Be vigilant against phone scams; Annual 'Dirty Dozen' list continues*. Retrieved from https://www.irs.gov/newsroom/irs-be-vigilant-against-phone-scams-annual-dirty-dozen-list-continues.

Internal Revenue Service. (2021). *IRS urges caution with email, social media and phones as part of "Dirty Dozen" series* . https://www.irs.gov/newsroom/irs-urges-caution-with-email-social-media-and-phones-as-part-of-dirty-dozen-series.

Kaniuk, R. S. (2016). Lawyer and IRS phishing e-mails become today's Nigerian e-mail scams. Experience: *The Magazine of the Senior Lawyers Division, American Bar Association, 26(3)*, 10.

Kantor, A. (2020). Would you fall for this £2,350 HMRC scam?. Retrieved 17 August 2020, from https://www.ft.com/taxscam.

Keatley, D. (2018). Crime Script Analysis. In. (Ed.), *Pathways in Crime* (pp. 125-136). Palgrave Macmillian.

Labrador, B., Ramón, N., Alaiz-Moretón, H., & Sanjurjo-González, H. (2014). Rhetorical structure and persuasive language in the subgenre of online advertisements. *English for Specific Purposes (New York, N.Y.), 34*, 3847. https://doi.org/10.1016/j.esp.2013.10.002.

Langenderfer, J., and Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology and Marketing, 18(7)*, 763–783. doi:10.1002/mar.1029.

Laroche, H., Steyer, V., & Theron, C. (2019). How Could You be so Gullible? Scams and Over-Trust in Organizations. *Journal of Business Ethics, 160*(1), 641-656. https://doi.org/10.1007/s10551-018-3941-z.

Lee, C. S. (2020). A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea. *Crime, Law and Social Change, 74*(1), 201-218. https://doi.org/10.1007/s10611-020-09885-3.

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

May, T., & Bhardwa, B. (2018). *Organised crime groups involved in fraud*. Cham: Palgrave Macmillan.

Ministry of Justice. (2017). Fraud and Scame. Retrieved 17 August 2020, from https://www.justice.gov.uk/help/fraud.

Moreto, W., & Clarke, R. (2013). 11 Script analysis of the transnational illegal market in endangered species. In B. Leclerc & R. Wortley, *Cognition and crime: Offender decision making and script analyses* (p. 209). Abingdon, Oxon: Routledge.

National Fraud Authority. (2013). *Annual fraud indicator June 2013* (p. 10). National Fraud Authority. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf.

National Fraud Authority. (2013). *Annual fraud indicator June 2013* (p. 10). National Fraud Authority. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf.

Office of Fair Trading (2006). Research on Impact of Mass Marketed Scams: A Summary of Research into the Impact of Scams on UK Consumers (No. OFT883). Office of Fair Trading: London.

Office for National Statistics (2016). *Overview of Fraud Statistics: Year ending March 2016.* Home Office. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016#how-is-fraud-defined-and-measured.

Office for National Statistics. (2019). *Crime in England and Wales: year ending December 2018*. Home Office. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2018.

Onyebadi, U., & Park, J. (2012). *'I'm sister maria. please help me': A lexical study of 4-1-9 international advance fee fraud email communications*. SAGE Publications. https://doi.org/10.1177/1748048511432602.

Osborne, J. R., & Capellan, J. A. (2017). Examining active shooter events through the rational choice perspective and crime script analysis. *Security journal*, *30*(3), 880-902.

Ownage Pranks. (2020). *15 Best IRS Scammer Numbers You Can Call!*. Ownage Pranks. https://www.ownagepranks.com/blog/irs-scammer-number-to-call-26/.

Protect yourself from tech support scams. (2019). Retrieved 28 September 2019, from https://support.microsoft.com/en-my/help/4013405/windows-protect-from-tech-support-scams.

Schaffer, D. (2012). The language of scam spams: linguistic features of "Nigerian fraud" e-mails. *ETC*, *69.2*. Retrieved from http://go.galegroup.com.manchester.idm.oclc.org/ps/i.do?id=GALE%7CA292237474&v=2.1&u=jrycal5&it=r&p=LitRC&sw=w.

Shover, N. (2003). Crime on the line: Telemarketing and the changing nature of professional crime. *British Journal Of Criminology*, *43*(3), 489-505. doi: 10.1093/bjc/43.3.489.

Schilling, N., and Marsters, A. (2015). Unmasking identity: Speaker profiling for forensic linguistic purposes. *Annual Review of Applied Linguistics*, *35*, 195–214. doi: 10.1017/s0267190514000282.

Schmidt, R., & Kess, J. F. (1986). *Television advertising and televangelism: Discourse analysis of persuasive language*. J. Benjamins Pub. Co.

Stebbins, R. A. (2001). *Exploratory research in the social sciences*. SAGE Publications, Inc. https://www.doi.org/10.4135/9781412984249.

Treasury Inspector General for Tax Administration. (2018). *TIGTA Semiannual Report to Congress: October 1, 2017 – March 31, 2018*. Washington: Department of the Treasury. Retrieved from https://www.treasury.gov/tigta/semiannual/semiannual_mar2018.pdf.

Tzani-Pepelasi C., Gavrilović Nilsson M., Lester D, Pylarinou R, N. & Ioannou., M. (2020). Profiling HMRC and IRS Scammers by Utilising Trolling Videos: Offender Characteristics. *Journal of Forensic and Investigative Accounting*. http://web.nacva.com/JFIA/Issues/JFIA-2020-No1-10.pdf.

UK Finance. (2019). *Fraud the facts 2019: The definitive overview of payment industry fraud*. UK Finance. Retrieved from https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf.

Watt, D. (2010). The identification of the individual through speech. In C. Llamas and D. Watt, *Language and identities* (1st ed., pp. 76–85). Edinburgh, Scotland: Edinburgh University Press. Retrieved from http://www- users.york.ac.uk/~dw539/watt2009.pdf.

Which?. (2020). How to spot HMRC phone, text and email tax scams. Retrieved 17 August 2020, from https://www.which.co.uk/consumer-rights/advice/how-to-spot-the-hmrc-tax-phone-scam.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: Perceived benefits and risk drive intention to comply in a mass marketing scam. *Journal Of Experimental Psychology: Applied*, *24*(2), 196-206. doi: 10.1037/xap0000167.